

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



542960

(43) Internationales Veröffentlichungsdatum
5. August 2004 (05.08.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/066219 A1

(51) Internationale Patentklassifikation⁷: G07B 15/00,
B60R 16/00, H04L 29/06

B SYSTEMS AG [DE/DE]; Öhderstrasse 4-4a, 42289
Wuppertal (DE).

(21) Internationales Aktenzeichen: PCT/EP2004/000505

(72) Erfinder; und

(22) Internationales Anmeldedatum:
22. Januar 2004 (22.01.2004)

(75) Erfinder/Anmelder (nur für US): KAMPERT, Werner
[DE/DE]; Alter Teichweg 9h, 22081 Hamburg (DE).
KNEE-FORREST, Paul [CZ/CZ]; Petra obravce 2261,
44001 Louny (CZ). BIEBER, Wolf-Rüdiger [DE/DE];
Brambecke 81, 42399 Wuppertal (DE). STAMM, Egbert
[DE/DE]; Küllersberg, 42653 Solingen (DE).

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 02 449.2 22. Januar 2003 (22.01.2003) DE
103 50 647.0 29. Oktober 2003 (29.10.2003) DE

(74) Anwalt: KARLHUBER, Mathias; Cohausz & Florack,
Bleichstrasse 14, 40211 Düsseldorf (DE).

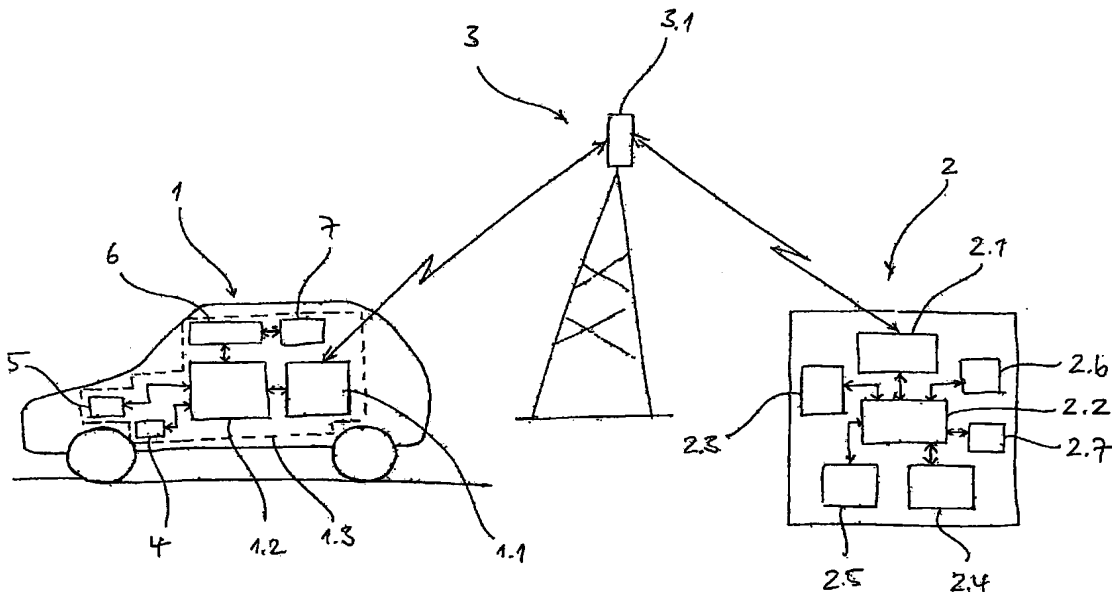
(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme
von US): FRANCOTYP-POSTALIA AG & CO. KG
[DE/DE]; Triftweg 21-26, 16547 Birkenwerder (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI,

[Fortsetzung auf der nächsten Seite]

(54) Title: MOBILE DATA TRANSMISSION METHOD AND SYSTEM

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR MOBILEN DATENÜBERTRAGUNG



(57) Abstract: The invention relates to a method for transmitting data between a mobile first device (1; 1', 1), particularly a vehicle, and a data center (2; 2') that is at least temporally remote from the first device (1; 1'; 1). The transmission of the data ensues over at least one mobile first transmission device (1.1; 1.1'; 1.1"), and the transmitted data contain first data that are authenticated by cryptographic means.

(57) Zusammenfassung: Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1"), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1") zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1") erfolgt und die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.

WO 2004/066219 A1



GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

- mit internationalem Recherchenbericht
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

(84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT,

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren und Anordnung zur mobilen Datenübertragung

Die vorliegende Erfindung betrifft ein Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale, wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung erfolgt. Sie betrifft weiterhin eine entsprechende Anordnung zum Übertragen von Daten.

Ein solches gattungsgemäßes Verfahren ist beispielsweise aus dem Bereich der Schienenverkehrstechnik bekannt. Dort werden zwischen dem Steuerrechner des Zuges über eine damit verbundene entsprechende Sender/Empfängereinheit des Zuges Daten mit einer externen Zugleitstelle ausgetauscht. Sofern es sich bei den ausgetauschten Daten um sicherheitsrelevante Daten handelt, wird durch entsprechend redundante Übertragungsprotokolle eine fehlerfreie Übertragung der die Daten repräsentierenden Signale sichergestellt bzw. werden nur solche Signale akzeptiert, deren Fehlerwahrscheinlichkeit innerhalb bestimmter Toleranzgrenzen liegt.

Ein Nachteil dieser bekannten Verfahren liegt darin, dass eine Absicherung der durch die Signale repräsentierten Daten gegen Manipulationen in der Regel nicht stattfindet. Bei der Übertragung der Daten zwischen dem Fahrzeug und der Datenzentrale könnte es somit problemlos zu wissentlichen und willentlichen Manipulationen kommen. Dies ist insbesondere dann von Nachteil, wenn diese Daten sicherheitsrelevante erste Daten umfassen. Um hier Manipulationen vorzubeugen, wäre es wünschenswert, eine entsprechende Absicherung solcher sicherheitsrelevanter erster Daten und damit einen Manipulationsschutz zu erzielen.

Weiterhin wäre es wünschenswert, das bekannte Verfahren auch in anderen Bereichen einsetzen zu können. Insbesondere wäre es wünschenswert, ein solches Verfahren bei der Überwachung anderer mobiler Einrichtungen einzusetzen. Hierzu zählt insbesondere die Überwachung von gemieteten oder geleasten Fahrzeugen. Gerade hier stellt sich aber wieder das Problem, dass die übertragenen Daten, gerade wenn sie beispielsweise abrechnungsrelevante und damit sicherheitsrelevante erste Daten umfassen, mit dem bekannten Datenübertragungsverfahren vergleichsweise anfällig für Manipulationen sind.

Der vorliegenden Erfindung liegt daher die Aufgabe zu Grunde, ein Verfahren bzw. eine Anordnung der eingangs genannten Art zur Verfügung zu stellen, welches bzw. welche die oben genannten Nachteile nicht oder zumindest in geringerem Maß aufweist und, insbesondere bei der Übertragung, einen erhöhten Manipulationsschutz sicherheitsrelevanter Daten gewährleistet.

Die vorliegende Erfindung löst diese Aufgabe ausgehend von einem Verfahren gemäß dem Oberbegriff des Anspruchs 1 durch die im kennzeichnenden Teil des Anspruchs 1 angegebenen Merkmale. Sie löst diese Aufgabe weiterhin ausgehend von einer Anordnung gemäß dem Oberbegriff des Anspruchs 17 durch die im kennzeichnenden Teil des Anspruchs 17 angegebenen Merkmale.

Der vorliegenden Erfindung liegt die technische Lehre zu Grunde, dass man einen erhöhten Manipulationsschutz sicherheitsrelevanter erster Daten erzielt, wenn die übertragenen ersten Daten durch kryptographische Mittel authentifiziert werden. Die Authentifizierung bringt den Vorteil mit sich, dass auch zu einem späteren Zeitpunkt durch ein entsprechendes Verifizierungsverfahren zweifelsfrei nachgewiesen werden kann, dass die Daten während der Übertragung oder gegebenenfalls auch später nicht manipuliert wurden.

Die Authentifizierung durch kryptographische Mittel kann in beliebiger bekannter Weise erfolgen. So kann beispielsweise ein so genannter Message Authentication Code (MAC) verwendet werden. Ein solcher MAC wird in der Regel unter Verwendung eines so genannten geteilten Geheimnisses, in der Regel eines geheimen Schlüssels generiert, der sowohl der den MAC erzeugenden Einheit als auch der den MAC verifizierenden Einheit bekannt ist, ansonsten aber geheim gehalten wird. Die zu authentifizierenden Daten werden zusammen mit dem geheimen Schlüssel einem Berechnungsalgorithmus zugeführt, der hieraus den MAC generiert. Der Berechnungsalgorithmus ist so ausgebildet, dass der MAC ohne Kenntnis des geheimen Schlüssels ohne übermäßig hohen Berechnungsaufwand nicht aus den zu authentifizierenden Daten rekonstruiert werden kann. Üblicherweise schließt der Berechnungsalgorithmus einen so genannten Hash-Algorithmus (z. B. SHA-1, SHA-2, MD5 etc.) ein. Zur Verifizierung des MAC wird seitens der verifizierenden Einheit aus den zu authentifizierenden Daten zusammen mit dem geheimen Schlüssel unter Verwendung des selben Berechnungsalgorithmus ein zweiter MAC gebildet, der dann mit dem MAC verglichen wird, der den zu authentifizierenden Daten zugeordnet ist. Stimmen diese überein, sind die Daten authentisch.

Wegen der einfacheren Verwaltung der verwendeten kryptographischen Schlüssel, insbesondere der einfacheren Verteilung der öffentlichen Schlüssel, beispielsweise im Rahmen einer so genannten Public Key Infrastruktur (PKI), werden zur Authentifizierung der Daten vorzugsweise digitale Signaturen verwendet. Hierbei verschlüsselt die Einheit, welche die digitale Signatur erzeugt, die zu authentifizierenden Daten oder einen daraus generierten Wert mit einem privaten Schlüssel, der in der Regel nur ihr bekannt ist. Um die den zu authentifizierenden Daten zugeordnete Signatur zu verifizieren und damit die Authentizität der Daten zu überprüfen, entschlüsselt die verifizierende Einheit die Signatur mit einem ihr bekannten öffentlichen Schlüssel, der dem privaten Schlüssel zugeordnet ist. Das Ergebnis der Entschlüsselung wird dann mit den zu authentifizierenden Daten oder einem Wert, der daraus nach dem bei der Verschlüsselung verwendeten Algorithmus generiert wurde. Stimmen diese überein, sind die Daten authentisch.

Bei den zu authentifizierenden ersten Daten kann es sich grundsätzlich um beliebige Daten handeln. So kann es sich um beliebige Daten handeln, die von entsprechenden Einrichtungen der ersten Einrichtung bzw. der Datenzentrale erfasst oder generiert wurden. Insbesondere kann es sich um beliebige Daten handeln, die von entsprechenden Erfassungseinrichtungen der mobilen ersten Einrichtung erfasst wurden. Hierzu zählen unter anderem beliebige Messdaten, die über beliebige Messeinrichtungen gemessen wurden.

Vorzugsweise wird zusammen mit diesen Daten auch ihre jeweilige Quelle authentifiziert.

Hierzu ist bevorzugt vorgesehen, dass die ersten Daten zur Authentifizierung einer ersten Quelle der ersten Daten wenigstens eine erste Quellenidentifikation umfassen. Diese erste Quellenidentifikation ist der ersten Quelle bevorzugt eindeutig zugeordnet. Es handelt sich vorzugsweise um eine einmalige und eindeutige Identifikation. Bei der ersten Quelle, die über die erste Quellenidentifikation identifiziert wird, kann es sich um die Einrichtung handeln, welche die ersten Daten erfasst bzw. generiert hat. So kann die erste Quelle beispielsweise ein Messaufnehmer oder Sensor sein, der die ersten Daten generiert. Ebenso kann es sich bei der ersten Quelle um eine Einrichtung handeln, über welche die ersten Daten im weiteren Verlauf geleitet werden. Dies ist insbesondere dann sinnvoll, wenn die ersten Daten durch diese Einrichtung eine Bearbeitung, eine Modifikation oder dergleichen erfahren. So kann die erste Quelle beispielsweise die Einrichtung sein, in der die ersten Daten authentifiziert werden. Ebenso kann es sich bei der ersten Quelle um eine Einrichtung handeln, über welche die ersten Daten übertragen werden.

Ein weiterer Vorteil dieser Variante liegt darin, dass durch die eindeutige Zuordnung der Daten zu der jeweiligen ersten Quelle anhand der authentifizierten Daten zu einem späteren

Zeitpunkt eine Aussage über die Qualität und die Leistungsfähigkeit der ersten Quelle getroffen werden kann. Dies gilt insbesondere dann, wenn eine längere Reihe von entsprechenden authentifizierten Daten zur Verfügung steht, sodass eine entsprechende Historie über die Leistung der ersten Quelle erstellt werden kann, aus der entsprechende Rückschlüsse gezogen werden können.

Die erste Quelle kann Bestandteil der ersten Einrichtung, der ersten Übertragungseinrichtung, der Datenzentrale oder jeder weiteren Einrichtung sein, über welche die Datenübertragung erfolgt. Vorzugsweise umfassen die ersten Daten jeweils eine Quellenidentifikation für sämtliche Stationen, welche die ersten Daten bei der Übertragung durchlaufen, um ihren Übertragungsweg zu einem späteren Zeitpunkt lückenlos nachvollziehen zu können.

Bei besonders vorteilhaften Ausgestaltungen des erfindungsgemäßen Verfahrens wird zudem auch der Empfänger der ersten Daten authentifiziert. Hierdurch ist es möglich, zu einem späteren Zeitpunkt den Nachweis zu führen, welche Daten an einen bestimmten Empfänger übergeben wurden. Dies ist insbesondere dann von Bedeutung, wenn der Empfang der ersten Daten die Erfüllung einer bestimmten entgeltspflichtigen Leistung darstellt. Durch die erfindungsgemäße Authentifizierung des Empfängers kann dann in vorteilhafter Weise zu einem späteren Zeitpunkt der Empfänger der ersten Daten und damit der Leistung nachgewiesen werden. Erfindungsgemäß ist hierzu bevorzugt vorgesehen, dass die ersten Daten zur Authentifizierung eines ersten Empfängers der ersten Daten eine erste Empfängeridentifikation umfassen.

Je nach Übertragungsrichtung kann der Empfänger Bestandteil der ersten Einrichtung, der ersten Übertragungseinrichtung, der Datenzentrale oder jeder weiteren Einrichtung sein, über welche die Datenübertragung erfolgt. Analog zu der oben geschilderten Quellenidentifikation ist vorzugsweise vorgesehen, dass die ersten Daten eine Empfängeridentifikation für jeden Empfänger aufweist, über den die Übertragung erfolgt. Bei Zwischenstationen in der Übertragung entspricht die Empfängeridentifikation dann in der Regel der Quellenidentifikation, sodass für solche Zwischenstationen lediglich eine einzige Identifikation in die ersten Daten aufgenommen werden muss.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahrens wird zusätzlich die Übertragung selbst bzw. ein Merkmal dieser Übertragung authentifiziert. Hierdurch ist es zu einem späteren Zeitpunkt möglich, gegebenenfalls nicht nur die Daten und die beteiligten Kommunikationspartner zweifelsfrei zu identifizieren. Es ist hiermit auch möglich, den Vorgang der Übertragung selbst zu identifizieren und/oder seine Qualität zu bewerten. So kann

die Übertragung beispielsweise durch ein entsprechendes zeitliches Merkmal in eine Reihenfolge von Übertragungen eingeordnet werden; um eine Historie der Übertragungen bzw. der übertragenen Daten zu erstellen. Ebenso kann die Übertragung durch ein entsprechendes Qualitätsmerkmal, beispielsweise das Signal-Rausch-Verhältnis, die Anzahl der Verbindungsversuche, Art und/oder Anzahl von aufgetretenen Fehlern etc., später hinsichtlich ihrer Qualität beurteilt werden. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten zur Authentifizierung der Übertragung der ersten Daten eine Übertragungsidentifikation umfassen. Diese Übertragungsidentifikation kann beispielsweise eine fortlaufende Übertragungsnummer umfassen, welche die Übertragung beispielsweise zusammen mit den Identifikationen der Kommunikationspartner eindeutig identifiziert. Eine exakte zeitliche Einordnung der Übertragung ist möglich, wenn die Übertragungsidentifikation eine absolute Zeitinformation hinsichtlich Beginn und/oder Ende der Übertragung umfasst.

Bei weiteren bevorzugten Varianten des erfindungsgemäßen Verfahrens werden zeitliche Ereignisse authentifiziert. Erfindungsgemäß umfassen die ersten Daten hierzu wenigstens eine für ein vorgebbares Ereignis charakteristische Zeitkennung. Bei den vorgebbaren Ereignis kann es sich beispielsweise um die Generierung bzw. Erfassung der zu übertragenen Daten handeln, ebenso kann es sich um das Senden bzw. Empfangen der ersten Daten handeln. Vorzugsweise ist jeweils eine Zeitkennung für einen dieser Vorgänge vorgesehen. Mit anderen Worten umfassen die ersten Daten beispielsweise eine erste Zeitkennung, die für den Zeitpunkt der Generierung bzw. Erfassung der zu übersenden Daten repräsentativ ist, eine zweite Zeitkennung, die für das Senden dieser Daten repräsentativ ist, und eine dritte Zeitkennung, die für das Empfangen dieser Daten repräsentativ ist.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass die authentifizierten ersten Daten in einen Protokolldatensatz eingefügt werden, der in der ersten Einrichtung und zusätzlich oder alternativ in der Datenzentrale gespeichert wird. Dieser Protokolldatensatz ermöglicht es gegebenenfalls beiden Kommunikationspartnern ohne weiteres zu einem beliebigen späteren Zeitpunkt die entsprechend authentifizierten Daten zu verifizieren.

Besonders günstige Varianten des erfindungsgemäßen Verfahrens zeichnen sich dadurch aus, dass mit ihnen eine zuverlässige Überwachung bestimmter Zustände, insbesondere bestimmter Zustände der mobilen ersten Einrichtung möglich ist. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer

ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung der ersten Einrichtung erfasst wurde.

Bei der Erfassungsgröße kann es sich grundsätzlich um eine beliebige durch entsprechende Erfassungseinrichtungen erfassende Größe handeln. So kann es sich beispielsweise um eine Zustandgröße der Umgebung der mobilen ersten Einrichtung handeln, welche durch entsprechende Sensoren oder dergleichen der mobilen ersten Einrichtung erfasst wird. Besonders vorteilhaft lässt sich das erfindungsgemäßen Verfahren jedoch zur Überwachung des Zustands der mobilen Einrichtung selbst einsetzen. Bevorzugt handelt es sich bei der ersten Erfassungsgröße daher um eine Zustandgröße der ersten Einrichtung. Diese Zustandgröße kann beispielsweise ein Betriebsparameter der ersten Einrichtung sein. Hierzu zählen beispielsweise die Geschwindigkeit und die Beschleunigung der ersten Einrichtung, die nach Betrag und Richtung erfasst werden können. Ebenso kann natürlich auch die Position der ersten Einrichtung die erste Erfassungsgröße bilden. Ebenso kann es sich um eine Temperatur handeln, wie z. B. die Temperatur im Kühlwasser- oder Motorölkreislauf etc. Schließlich kann es sich um einen Ölstand, den Reifendruck oder einen beliebigen anderen Zustandsparameter handeln. Es versteht sich im übrigen, dass beliebige Kombinationen solche Erfassungsgrößen über entsprechende Erfassungseinrichtungen erfasst und übermittelt werden können, um den Zustand der ersten Einrichtung zu charakterisieren.

Weitere vorteilhafte Varianten des erfindungsgemäßen Verfahrens ermöglichen eine Beeinflussung bestimmter Betriebsparameter und damit des Betriebs der mobilen ersten Einrichtung. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten wenigstens Betriebsbeeinflussungsdaten umfassen, die zur Beeinflussung des Betriebs der ersten Einrichtung an die erste Einrichtung übermittelt werden. So ist es beispielsweise möglich, durch die Übertragung der ersten Daten zur ersten Einrichtung aktuelle Betriebsparameter zu verändern. Ebenso kann beispielsweise ein Austausch von Teilen der Betriebssoftware der ersten Einrichtung bis hin zum kompletten Austausch der Betriebssoftware vorgenommen werden. Mit der erfindungsgemäßen Authentifizierung der ersten Daten kann, gegebenenfalls zusammen mit anderen Sicherungsmechanismen, sichergestellt werden, dass nur authentische und autorisierte Daten berücksichtigt werden. Es kann damit also mit anderen Worten nur zu einer autorisierten Beeinflussung des Betriebs der mobilen ersten Einrichtung erfolgen.

Bei weiteren vorteilhaften Varianten des erfindungsgemäßen Verfahrens werden die Daten über wenigstens eine zweite Datenübertragungseinrichtung übertragen. Diese zweite Datenübertragungseinrichtung kann sowohl ebenfalls mobil als auch stationär sein. Hierdurch

ist es möglich, ein kostengünstiges Übertragungssystem zu realisieren. So kann die zweite Datenübertragungseinrichtung entsprechend leistungsfähig ausgebildet sein, um die ersten Daten über eine weite Strecke zu und von der Datenzentrale zu übertragen. Die erste Datenübertragungseinrichtung kann dann einfacher und kostengünstiger gestaltet werden. Insbesondere kann sie für eine kürzere Übertragungsstrecke zur zweiten Datenübertragungseinrichtung ausgelegt werden. In einem solchen System kann beispielsweise ein ausreichend flächendeckendes Netz von zweiten Datenübertragungseinrichtungen realisiert werden, wobei sich eine erste Datenübertragungseinrichtung und eine zweite Datenübertragungseinrichtung dann lediglich ausreichend nahe kommen müssen, um die Übertragung zwischen der mobilen ersten Einrichtung der entfernten Datenzentrale sicherzustellen.

Die vorliegende Erfindung betrifft weiterhin ein Verfahren zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, bei dem zwischen der mobilen ersten Einrichtung und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale über wenigstens eine mobile erste Übertragungseinrichtung erste Daten mit dem oben beschriebenen erfindungsgemäßen Verfahren übertragen werden. Erfindungsgemäß umfassen die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten. Die ersten Überwachungsdaten umfassen wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße, der von einer ersten Erfassungseinrichtung der ersten Einrichtung erfasst wurde. Diese ersten Überwachungsdaten werden in der Datenzentrale verifiziert. Schließlich werden die ersten Überwachungsdaten bei erfolgreicher Verifikation in der Datenzentrale analysiert.

Vorzugsweise wird in der Datenzentrale in Abhängigkeit von der Analyse der ersten Überwachungsdaten eine erste Überwachungsreaktion ausgelöst. Bei der Überwachungsreaktion kann es sich grundsätzlich um eine beliebige Reaktion handeln.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahren handelt es sich bei der Überwachungsreaktion um eine Abrechnung handeln. So kann beispielsweise bei der Überwachung der Nutzung von gemieteten oder geleasten mobilen Einheiten, beispielsweise Fahrzeugen, Baumaschinen etc., in Abhängigkeit von der über entsprechende Erfassungseinrichtungen erfassten, übermittelten und analysierten abrechnungsrelevanten Nutzung eine Abrechnung der Nutzung erfolgen. Durch die erfindungsgemäße Authentifizierung der übermittelten Daten ist dabei sichergestellt, dass diese während der Übertragung nicht manipuliert wurden. Erfindungsgemäß ist hierzu vorgesehen, dass die erste Überwachungsreaktion einen Abrechnungsvorgang umfasst.

Zusätzlich oder alternativ können auch beliebige andere Überwachungsreaktionen ausgelöst werden. So können beispielsweise im Rahmen der Überwachung des Betriebszustands von mobilen Einrichtungen so genannte Frühwarnsysteme realisiert werden. Werden beispielsweise über die ersten Daten Fehler oder kritische Zustände bestimmter Einheiten der ersten
5 Einrichtung erfasst oder ergibt sich aus der Analyse der ersten Daten, dass derartige Fehler oder kritische Zustände, gegebenenfalls mit einer bestimmten Wahrscheinlichkeit, innerhalb eines bestimmten Zeitraums eintreten, so kann als Überwachungsreaktion eine entsprechende Mitteilung an die erste Einrichtung übermittelt werden. Die erste Einrichtung kann diese Nachricht dann an den aktuellen Nutzer über eine entsprechend Schnittstelle, beispielsweise optisch und/oder akustisch ausgeben. Es versteht sich, dass diese Nachricht
10 dabei in der oben beschriebenen Weise entsprechend authentifiziert übermittelt werden kann, um Manipulationen auszuschließen. Zusätzlich oder alternativ kann eine solche Nachricht von der Datenzentrale auch automatisch, beispielsweise per Mobilfunk, an einen entsprechend registrierten Nutzer übermittelt werden.

15 Es versteht sich jedoch, dass nicht nur für die Funktion der mobilen Einheit unmittelbar relevante Erfassungsgrößen erfasst werden können. Mit anderen Worten können beispielsweise auch andere Erfassungsgrößen erfasst werden, welche keinen unmittelbaren Einfluss auf die Funktionsfähigkeit der mobilen Einheit haben.

So kann beispielsweise im Fall von gemieteten oder geleasten mobilen Einheiten die aktuelle Nutzung überwacht werden und als eine Überwachungsreaktion eine entsprechende
20 Nachricht generiert werden, sobald der Nutzer den vereinbarten Nutzungsrahmen überschreitet oder zu überschreiten droht. Ebenso kann bei Überschreiten des vereinbarten Nutzungsrahmens als Überwachungsreaktion auf einen anderen Abrechnungsmodus umgeschaltet werden. War beispielsweise bei einem gemieteten Fahrzeug eine bestimmte Kilometerleistung pauschal vergütet, kann bei Erfassung des Überschreitens dieser Kilometerleistung auf eine kilometerbezogene Abrechnung der Mehrkilometer umgeschaltet werden.
25

Ebenso kann beispielsweise gemieteten oder geleasten Fahrzeugen oder Maschinen die Position als erste Erfassungsgröße überwacht und analysiert werden. Verstößt der Nutzer gegen eine Vereinbarung, indem das Fahrzeug beispielsweise einen vereinbarten Einsatzbereich verlässt, oder droht ein solcher Verstoß, so kann ebenfalls eine entsprechende
30 Nachricht bzw. Warnung als Überwachungsreaktion übermittelt werden.

Weiterhin kann beispielsweise im Rahmen der Überwachung vorgeschriebener Ruhezeiten für Fahrzeugführer die Betriebsdauer anhand entsprechender Kriterien überwacht werden.

Ergibt sich anhand einer oder mehrerer Erfassungsgrößen, dass die vorgeschriebenen Ruhezeiten nicht eingehalten werden bzw. ein Verstoß hiergegen droht, so kann ebenfalls eine entsprechende Nachricht bzw. Warnung als Überwachungsreaktion übermittelt werden.

Der beiden vorgenannten Fällen können im Fall des Verstoßes unter bestimmten Voraussetzungen als weitere Überwachungsreaktion Gegenmaßnahmen eingeleitet werden. Im einfachsten Fall kann dies durch eine entsprechende Mitteilung an eine hoheitliche Einrichtung, wie beispielsweise die Polizei oder dergleichen, übermittelt werden, um den Verstoß abzustellen.

Ebenso kann aber unter Berücksichtigung entsprechender Sicherheitsvorschriften als Überwachungsreaktion eine direkte Beeinflussung der ersten Einrichtung erfolgen. Diese kann gegebenenfalls bis hin zur kontrollierten Abschaltung der ersten Einrichtung reichen.

Eine solche Beeinflussung kann natürlich auch im Fall der oben genannten Überwachung funktionsrelevanter Erfassungsgrößen erfolgen. Vorzugsweise ist daher vorgesehen, dass die erste Überwachungsreaktion die Generierung von Betriebsbeeinflussungsdaten umfasst, die zur Beeinflussung des Betriebs der ersten Einrichtung an die erste Einrichtung übermittelt werden. Wird beispielsweise erfasst, dass für einen bestimmten Betriebsparameter ein kritischer Zustand droht oder vorliegt, können unter Berücksichtigung entsprechender Sicherheitsvorschriften entsprechende Gegenmaßnahmen eingeleitet werden, um diesen kritischen Zustand zu verhindern oder abzustellen. Hierbei ist es unter anderem auch möglich, schadhafte Betriebssoftware oder Teile über eine solche Betriebsbeeinflussung zu warten oder gegebenenfalls sogar vollständig auszutauschen.

In allen vorgenannten Fällen mit entsprechenden Überwachungsreaktionen stellt die Authentifizierung der im Rahmen der Überwachungsreaktion an die mobile Einheit übermittelten ersten Daten sicher, dass es im Rahmen einer solchen Überwachungsreaktion zu keinen nicht autorisierten Manipulationen kommen kann, sondern lediglich Prozesse ablaufen, die auf entsprechend autorisierten Daten basieren.

Bei weiteren bevorzugten Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass bei der Analyse weitere, nicht von der ersten Einrichtung übermittelte Daten berücksichtigt werden. Hierbei kann es sich beispielsweise um statistische Daten handeln, welche durch die Auswertung der Daten gewonnen wurden, die von baugleichen oder ähnlichen ersten Einrichtungen stammen. Ebenso kann es sich aber um, auf anderem Wege zu Datenzentrale gelangte Daten handeln. Insbesondere können bei der Auslösung einer Überwachungsreaktion auch externe Informationen hinsichtlich der ersten Einrichtung berücksichtigt

werden. So kann zum Beispiel eine der oben beschriebenen Überwachungsreaktionen ausgelöst werden, wenn in der Datenzentrale eine Information eingeht, dass die erste Einrichtung gestohlen wurde oder dergleichen.

- Die vorliegende Erfindung betrifft weiterhin eine Anordnung zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale, wobei zur Übertragung der Daten wenigstens eine mobile erste Übertragungseinrichtung vorgesehen ist. Erfindungsgemäß umfassen die übertragenen Daten erste Daten und es ist wenigstens eine Sicherheitseinrichtung vorgesehen, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist. Die erfindungsgemäße Anordnung eignet sich zur Durchführung des erfindungsgemäßen Verfahrens. Mit ihr lassen sich die vorstehend beschriebenen Ausgestaltungen und Vorteile in derselben Weise realisieren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird.
- 15 Die Sicherheitseinrichtung umfasst dabei ein Kryptographiemodul, welches die oben beschriebenen kryptographischen Mittel zur Verfügung stellt. Die Sicherheitseinrichtung kann dabei insbesondere zur oben beschriebenen Generierung eines MAC ausgebildet sein. Vorzugsweise ist die Sicherheitseinrichtung zur Bildung einer ersten digitalen Signatur unter Verwendung der ersten Daten ausgebildet, um die ersten Daten zu authentifizieren.
- 20 Das Kryptographiemodul kann sowohl zur Verschlüsselung zu speichernder Daten verwendet werden als auch zur Verschlüsselung zu übertragender Daten. Es versteht sich, dass je nach Anwendung, also beispielsweise je nachdem, ob Daten versandt oder gespeichert werden sollen, auch unterschiedliche kryptographische Verfahren angewendet werden können.
- 25 Neben dem bzw. den kryptographischen Algorithmen und einem oder mehreren entsprechenden kryptographischen Schlüsseln umfassen die Kryptographiedaten das Kryptographiemoduls bevorzugt weitere Daten, wie beispielsweise ein oder mehrere kryptographische Zertifikate entsprechender Zertifizierungsinstanzen sowie gegebenenfalls ein oder mehrere eigene kryptographische Zertifikate der Sicherheitseinrichtung.
- 30 Vorzugsweise ist die Sicherheitseinrichtung zum Austausch wenigstens eines Teils der Kryptographiedaten ausgebildet, um in vorteilhafter Weise eine einfache und dauerhaft zuverlässige Sicherung der Daten zu gewährleisten. Hierbei kann insbesondere vorgesehen sein, dass neben den kryptographischen Schlüsseln und kryptographischen Zertifikaten

auch der jeweils verwendete kryptographische Algorithmus ausgetauscht werden kann, um das System in einfacher Weise an geänderte Sicherheitsanforderungen anpassen zu können. Die Implementierung und der Austausch der Kryptographiedaten erfolgt bevorzugt im Rahmen einer so genannten Public Key Infrastruktur (PKI), wie sie hinlänglich bekannt ist und daher an dieser Stelle nicht weiter beschrieben werden soll. Es versteht sich insbesondere, dass eine entsprechende Routine zur Überprüfung der Validität der verwendeten kryptographischen Zertifikate vorgesehen ist. Geeignete derartige Überprüfungsrou-
tinen sind ebenfalls hinlänglich bekannt und sollen daher hier nicht näher beschrieben werden

Vorzugsweise ist die Sicherheitseinrichtung zur oben beschriebenen Authentifizierung einer ersten Quelle der ersten Daten ausgebildet. Hierzu ist die Sicherheitseinrichtung bevorzugt zum Einbringen einer ersten Quellenidentifikation in den ersten Datensatz ausgebildet. Weiter vorzugsweise ist die Sicherheitseinrichtung zur oben beschriebenen Authentifizierung eines ersten Empfängers der ersten Daten ausgebildet. Hierzu ist sie vorzugsweise zum Einbringen einer ersten Empfängeridentifikation in den ersten Datensatz ausgebildet.

Bei bevorzugten Varianten der erfindungsgemäßen Anordnung ist die Sicherheitseinrichtung zur Authentifizierung der Übertragung der ersten Daten ausgebildet. Hierzu ist sie bevorzugt zum Einbringen einer Übertragungsidentifikation in den ersten Datensatz ausgebildet. Weiterhin ist die Sicherheitseinrichtung vorzugsweise zum Einbringen wenigstens einer für ein vorgebbares Ereignis charakteristischen Zeitkennung in den ersten Datensatz ausgebildet.

Bei weiteren vorteilhaften Varianten der erfindungsgemäßen Anordnung ist vorgesehen, dass die Sicherheitseinrichtung zum Einbringen der authentifizierten ersten Daten in einen Protokolldatensatz ausgebildet ist. Die erste Einrichtung weist dann einen ersten Protokollspeicher zum Speichern des Protokolldatensatzes auf. Zusätzlich oder alternativ weist die Datenzentrale einen zweiten Protokollspeicher zum Speichern des Protokolldatensatzes auf.

Die Sicherheitseinrichtung kann grundsätzlich an beliebiger Stelle in der Übertragungsstrecke angeordnet sein. Bevorzugt umfasst die erste Einrichtung eine erste derartige Sicherheitseinrichtung. Zusätzlich oder alternativ umfasst die Datenzentrale eine zweite derartige Sicherheitseinrichtung.

Bei vorteilhaften Varianten der erfindungsgemäßen Anordnung umfassen die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten. Diese Überwachungsdaten umfassen wiederum wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße. Die erste Einrichtung umfasst weiterhin eine erste Erfassungsein-

richtung zur Erfassung des ersten Erfassungswerts. Bei den Erfassungsgrößen kann es sich, wie oben erwähnt, um beliebige erfassbare Größen handeln. Bevorzugt ist die erste Erfassungseinrichtung zur Erfassung einer Zustandsgröße der ersten Einrichtung als erster Erfassungsgröße ausgebildet.

- 5 Bei weiteren bevorzugten Varianten der erfindungsgemäßen Anordnung ist vorgesehen, dass die ersten Daten von der Datenzentrale zur ersten Einrichtung übertragene Betriebsbeeinflussungsdaten umfassen. Die erste Einrichtung umfasst dann eine Betriebsbeeinflussungseinrichtung, um hierüber den Betrieb der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten zu beeinflussen, wie dies oben im Zusammenhang mit dem
- 10 erfindungsgemäßen Verfahren beschrieben wurde.

Die vorliegende Erfindung betrifft weiterhin eine Anordnung zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, mit einer erfindungsgemäßen Anordnung zur Übertragung von ersten Daten. Die ersten Daten umfassen dabei von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten, die wenigstens einen

15 ersten Erfassungswert einer ersten Erfassungsgröße umfassen. Die erste Einrichtung umfasst weiterhin eine erste Erfassungseinrichtung zur Erfassung des ersten Erfassungswerts. Die Datenzentrale weist eine zweite Sicherheitseinrichtung zum Verifizieren der ersten Überwachungsdaten auf. Weiterhin weist die Datenzentrale eine mit der zweiten Sicherheitseinrichtung verbundene Analyseeinrichtung zum Analysieren der ersten Überwachungsdaten in Abhängigkeit vom Ergebnis der Verifikation auf. Diese erfindungsgemäße Anordnung

20 eignet sich zur Durchführung des erfindungsgemäßen Verfahrens zur Überwachung einer mobilen ersten Einrichtung. Mit ihr lassen sich die vorstehend beschriebenen Ausgestaltungen und Vorteile in derselben Weise realisieren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird.

- 25 Bevorzugt ist wenigstens eine mit der Analyseeinrichtung verbindbare Überwachungsreaktionseinrichtung zur Durchführung einer ersten Überwachungsreaktion vorgesehen. Die Analyseeinrichtung ist dann zum Ansteuern der Überwachungsreaktionseinrichtung ausgebildet, um eine erste Überwachungsreaktion in Abhängigkeit vom Ergebnis der Analyse der ersten Überwachungsdaten auszulösen.

- 30 Vorzugsweise ist als Überwachungsreaktionseinrichtung eine mit der Analyseeinrichtung verbindbare Abrechnungseinrichtung vorgesehen. Weiter vorzugsweise ist die Überwachungsreaktionseinrichtung zur Generierung von Betriebsbeeinflussungsdaten als erste Überwachungsreaktion ausgebildet, wobei Betriebsbeeinflussungsdaten die zur Beeinflus-

sung des Betriebs der ersten Einrichtung dienen. Die Datenzentrale ist dann zur Übertragung erster Daten an die erste Einrichtung ausgebildet, wobei die ersten Daten die Betriebsbeeinflussungsdaten umfassen. Schließlich weist die erste Einrichtung eine Betriebsbeeinflussungseinrichtung zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten auf.

Bei weiteren bevorzugten Varianten der erfindungsgemäßen Anordnung umfasst die erste Einrichtung eine erste Sicherheitseinrichtung, die zum Verifizieren der die Betriebsbeeinflussungsdaten umfassenden ersten Daten ausgebildet ist. Die Betriebsbeeinflussungseinrichtung ist dann zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit vom Ergebnis der Verifizierung ausgebildet.

Die vorliegende Erfindung betrifft weiterhin eine mobile erste Einrichtung, insbesondere Fahrzeug, für eine erfindungsgemäße Anordnung. Erfindungsgemäß umfasst die erste Einrichtung eine erste Datenübertragungseinrichtung zur Übertragung erster Daten und eine mit der ersten Datenübertragungseinrichtung verbindbare erste Sicherheitseinrichtung. Die Sicherheitseinrichtung ist zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet.

Bei einer bevorzugten Ausgestaltung der erfindungsgemäßen mobilen Einrichtung ist die erste Sicherheitseinrichtung zur Authentifizierung der ersten Datenübertragungseinrichtung ausgebildet. Hierzu ist sie bevorzugt zum Einbringen einer der ersten Datenübertragungseinrichtung zugeordneten Identifikation in den ersten Datensatz ausgebildet.

Die vorliegende Erfindung betrifft schließlich eine Datenzentrale für eine erfindungsgemäße Anordnung. Erfindungsgemäß weist die Datenzentrale eine Datenübertragungseinrichtung zur Übertragung erster Daten und eine mit der Datenübertragungseinrichtung verbindbare zweite Sicherheitseinrichtung auf, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

Um erhöhten Schutz vor unerkannter unbefugter Manipulation der gespeicherten ersten Daten, insbesondere der gespeicherten Erfassungswerte zu erzielen, ist die jeweilige Sicherheitseinrichtung bevorzugt zur Überprüfung der Zugriffsberechtigung auf wenigstens einen Teil der Sicherheitseinrichtung oder anderer Teile der ersten Einrichtung bzw. der Datenzentrale ausgebildet. Die Überprüfung kann sich dabei auf einzelne, entsprechend sicherheitsrelevante Bereiche der Sicherheitseinrichtung beschränken. Sie kann sich jedoch

auch auf die Überprüfung der Zugriffsberechtigung für sämtliche Bereiche der Sicherheitseinrichtung erstrecken.

Bevorzugt wird schon die Zugriffsberechtigung auf den Speicher überprüft, in dem die ersten Daten gespeichert sind, um den unberechtigten Zugriff auf die ersten Daten zu verhindern.

5 Es versteht sich jedoch, dass bei bestimmten Varianten der erfindungsgemäßen Anordnung der Zugriff auf den Speicher für die ersten Daten auch ohne besondere Zugriffsberechtigung zugelassen sein kann, wenn die ersten Daten bereits in entsprechend authentifizierter Weise gespeichert sind, dass nicht autorisierte Manipulationen an den ersten Daten erkennbar sind. Dies ist der Fall, wenn die ersten Daten beispielsweise bereits zusammen mit einer
10 unter Verwendung der ersten Daten erzeugten Authentifizierungsinformation, wie beispielsweise einem obengenannten MAC, einer digitalen Signatur oder dergleichen gespeichert sind. Die Authentifizierungsinformation wird dann bevorzugt, in einem Bereich der Sicherheitseinrichtung erzeugt, für den die Zugriffsberechtigung, sofern der Zugriff überhaupt möglich ist, überprüft wird.

15 Hierdurch wird erreicht, dass eine unbefugte Manipulation des gespeicherten ersten Daten zum einen entweder mangels Zugriff auf die ersten Daten überhaupt nicht möglich ist oder bei einer Überprüfung zumindest nicht unerkannt bleibt.

Die Überprüfung der Zugriffsberechtigung kann grundsätzlich in beliebiger geeigneter Weise erfolgen. So ist es beispielsweise möglich, ein Passwortsystem oder dergleichen zu implementieren. Bevorzugt ist vorgesehen, dass die Verarbeitungseinheit zur Überprüfung der
20 Zugriffsberechtigung unter Einsatz kryptographischer Mittel ausgebildet ist. Hierbei können beispielsweise digitale Signaturen und kryptographische Zertifikate zur Anwendung kommen. Dies ist von besonderem Vorteil, da derartige kryptographische Verfahren einen besonders hohen Sicherheitsstandard gewährleisten.

25 Hierbei können im übrigen wenigstens zwei unterschiedliche Zugriffsberechtigungsstufen vorgesehen sein, die mit unterschiedlichen Zugriffsrechten auf die Sicherheitseinrichtung bzw. mit ihr verbundenen Einrichtungen verknüpft sind. Hiermit lässt sich in einfacher Weise zum einen eine hierarchische Struktur mit unterschiedlich weit gehenden Zugriffsrechten implementieren. So kann beispielsweise dem Benutzer der Anordnung auf der untersten
30 Zugriffsberechtigungsstufe als einzige Zugriffshandlung erlaubt sein, die gespeicherten ersten Daten auszulesen, während einem Administrator auf einer höheren Zugriffsberechtigungsstufe neben dem Auslesen der ersten Daten gegebenenfalls die Modifikation weiterer Komponenten der Sicherheitseinrichtung etc. möglich ist.

Zum anderen lässt sich über die Zugriffsberechtigungsstufen auf derselben Hierarchieebene aber auch der Zugriff auf unterschiedliche Bereiche der Sicherheitseinrichtung bzw. mit ihr verbundenen Einrichtungen steuern. Die Anzahl der Zugriffsberechtigungsstufen oder Klassen richtet sich dabei nach der jeweiligen Verwendung der Anordnung und der Komplexität der mit der erfindungsgemäßen Anordnung realisierbaren Anwendungen.

Bei bevorzugten Ausgestaltungen der erfindungsgemäßen Anordnung werden die ersten Erfassungswerte verknüpft mit einer für den Erfassungszeitpunkt des ersten Erfassungswerts charakteristischen Erfassungszeitkennung ausgebildet. Durch diese häufig auch als Zeitstempel bezeichnete Verknüpfung des gespeicherten ersten Erfassungswerts mit dem Zeitpunkt seiner Erfassung wird die Weiterverarbeitung des Erfassungswerts, beispielsweise zu Zwecken der Abrechnung aber auch zu Zwecken der Statistik etc. deutlich erleichtert. Dies gilt insbesondere dann, wenn mehrere, zu unterschiedlichen Zeiten erfasste erste Erfassungswerte verarbeitet werden sollen.

Es versteht sich jedoch, dass es bei anderen Varianten der Erfindung ohne derartige Zeitstempel auch ausreichen kann, wenn lediglich durch geeignete Maßnahmen sichergestellt ist, dass die Chronologie der Erfassung der ersten Erfassungswerte nachvollziehbar ist. So können den ersten Erfassungswerten beispielsweise fortlaufende Nummern zugeordnet werden, um dieses Ziel zu erreichen.

Die Ermittlung der Erfassungszeit kann auf beliebige geeignete Weise erfolgen. Bevorzugt umfasst die Sicherheitseinrichtung zur Ermittlung der Erfassungszeitkennung ein mit der Verarbeitungseinheit verbundenes Zeiterfassungsmodul. Hierbei kann es sich um eine integrierte Echtzeituhr handeln oder ein Modul, das über eine geeignete Kommunikationsverbindung zu einer entsprechenden Instanz die Echtzeit abfragt. Die integrierte Echtzeituhr kann dabei gegebenenfalls von Zeit zu Zeit mit einer entsprechend genauen Zeitquelle synchronisiert werden.

Bei besonders günstigen Varianten der Erfindung ist wenigstens eine zweite Erfassungseinrichtung zur Erfassung wenigstens eines zweiten Erfassungswerts der ersten Erfassungsgröße vorgesehen. Mit diesen Varianten ist es möglich, auch größere Systeme mit mehreren Erfassungsorten der Erfassungsgröße, beispielsweise mehreren Messstellen für den Verbrauch eines Verbrauchsgutes, mit einer reduzierten Anzahl von Sicherheitseinrichtungen, gegebenenfalls sogar mit einer einzigen Sicherheitseinrichtung zu betreiben. Um die Trennung der ersten und zweiten Erfassungswerte sicherzustellen, kann vorgesehen sein, dass die ersten und zweiten Erfassungswerte in unterschiedlichen Speicherbereichen abgelegt

werden. Hierbei können insbesondere unterschiedliche Zugriffsberechtigungen für die unterschiedlichen Speicherbereiche definiert sein, um sicherzustellen, dass nur die jeweils autorisierten Personen bzw. Einrichtungen auf den entsprechenden Speicherbereich zugreifen können.

- 5 Besonders vorteilhaft ist es jedoch, wenn der erste Erfassungswert verknüpft mit einer für die erste Erfassungseinrichtung charakteristischen ersten Erfassungseinrichtungskennung und der zweite Erfassungswert verknüpft mit einer für die zweite Erfassungseinrichtung charakteristischen zweiten Erfassungseinrichtungskennung gespeichert wird. Mit dieser eindeutigen Zuordnung zwischen der Erfassungseinrichtung und dem durch sie erfassten Erfassungswerts ist eine besonders einfache und zuverlässige Trennung möglich, welche die
10 spätere Weiterverarbeitung erheblich erleichtert.

- Bei weiteren günstigen Ausgestaltungen der erfindungsgemäßen Anordnung ist vorgesehen, dass die erste Erfassungseinrichtung zur Erfassung wenigstens eines dritten Erfassungswerts einer zweiten Erfassungsgröße ausgebildet ist. Alternativ kann eine dritte Erfassungseinrichtung zur Erfassung wenigstens eines dritten Erfassungswerts einer zweiten Erfassungsgröße vorgesehen sein. Hierdurch ist es möglich, mit einer einzigen Sicherheitseinrichtung die Erfassung und gesicherte Speicherung der Erfassungswerte für unterschiedliche Erfassungsgrößen zu realisieren.
15

- Um die Trennung der ersten und dritten Erfassungswerte sicherzustellen, kann auch hier
20 wieder vorgesehen sein, dass die ersten und dritten Erfassungswerte in unterschiedlichen Speicherbereichen abgelegt werden. Besonders vorteilhaft ist es jedoch auch hier, wenn der erste Erfassungswert verknüpft mit einer für die erste Erfassungsgröße charakteristischen ersten Erfassungsgrößenkennung und der dritte Erfassungswert verknüpft mit einer für die zweite Erfassungsgröße charakteristischen zweiten Erfassungsgrößenkennung gespeichert
25 wird. Mit dieser eindeutigen Zuordnung zwischen der Erfassungseinrichtung und der durch sie erfassten Erfassungsgröße ist eine besonders einfache und zuverlässige Trennung möglich, welche die spätere Weiterverarbeitung der gespeicherten Daten erheblich erleichtert.

- Bei bevorzugten Varianten der erfindungsgemäßen Anordnung sind die erste Erfassungseinrichtung und die Sicherheitseinrichtung in einer vor unbefugtem Zugriff geschützten sicheren
30 Umgebung angeordnet, um in vorteilhafter Weise den unbefugten Zugriff nicht nur auf die Daten der Sicherheitseinrichtung sondern auch auf die Daten, die von und zu der ersten Erfassungseinrichtung geliefert werden, wirksam zu unterbinden.

Die sichere Umgebung kann dabei physisch durch ein oder mehrere entsprechend gesicherte Gehäuse hergestellt werden. Diese Gehäuse sind dann bevorzugt mit entsprechenden, hinlänglich bekannten Mitteln zur Erfassung von Manipulationen am Gehäuse ausgestattet. Bevorzugt erfolgt die Sicherung jedoch auch logisch durch ein entsprechend abgesichertes Kommunikationsprotokoll zwischen der ersten Erfassungseinrichtung und der Sicherheitseinrichtung. So kann beispielsweise vorgesehen sein, dass bei jeder Kommunikation zwischen der ersten Erfassungseinrichtung und der Sicherheitseinrichtung über eine entsprechend starke gegenseitige Authentifizierung ein gesicherter Kommunikationskanal aufgebaut wird. Es versteht sich, dass die erste Erfassungseinrichtung in diesem Fall über entsprechende Kommunikationsmittel verfügt, welche die beschriebene Sicherheitsfunktionalität zur Verfügung stellen.

Es versteht sich weiterhin, dass die sichere Umgebung durch solche logischen Sicherungsmechanismen auf einen beliebig großen Raum erstreckt werden kann. So können die erste Erfassungseinrichtung und die Sicherheitseinrichtung bei solchen Ausführungen innerhalb der sicheren Umgebung weit voneinander entfernt angeordnet sein. Es versteht sich weiterhin, dass die sichere Umgebung durch solche logischen Sicherungsmechanismen auch auf andere Komponenten, beispielsweise das Datenzentrum, ausgeweitet werden kann.

Es versteht sich, dass sämtliche der oben beschriebenen Module und Funktionen der Sicherheitseinrichtung durch entsprechend gestaltete Hardwaremodule realisiert sein können. Bevorzugt sind sie jedoch zumindest zum Teil als Softwaremodule gestaltet, auf welche die Verarbeitungseinheit zugreift, um die entsprechende Funktion zu realisieren. Weiterhin versteht es sich, dass die einzelnen Speicher nicht durch getrennte Speichermodule realisiert sein müssen. Vielmehr handelt es sich bevorzugt um entsprechend logisch getrennte Speicherbereiche eines einzigen Speichers, beispielsweise eines einzigen Speichermoduls.

Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen bzw. der nachstehenden Beschreibung eines bevorzugten Ausführungsbeispiels, welche auf die beigefügten Zeichnungen Bezug nimmt. Es zeigen

Figur 1 eine schematische Darstellung einer bevorzugten Ausführungsform der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens;

Figur 2 ein Blockschaltbild von Komponenten der Anordnung aus Figur 1;

Figur 3 eine schematische Darstellung einer weiteren bevorzugten Ausführungsform der erfindungsgemäßen Anordnung;

Figur 4 eine schematische Darstellung einer weiteren bevorzugten Ausführungsform der erfindungsgemäßen Anordnung.

5 Figur 1 zeigt ein bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens zur Übertragung von Daten zwischen einer mobilen ersten Einrichtung in Form eines Fahrzeugs 1 und einer davon entfernten Datenzentrale 2. Bei dem Fahrzeug 1 handelt es sich im vorliegenden Beispiel um einen Mietwagen. Die vorliegende Erfindung wird hierbei im Zusammenhang mit der Überwachung
10 und insbesondere mit der Abrechnung für die Nutzung dieses Mietwagens eingesetzt.

Das Fahrzeug 1 umfasst eine mobile erste Übertragungseinrichtung in Form eines ersten Mobilfunkmoduls 1.1 für ein Mobilfunknetz 3. Mittels des Mobilfunkmoduls 1.1 können Daten über eine zweite Übertragungseinrichtung 3.1 des Mobilfunknetzes 3 mit einer dritten Übertragungseinrichtung in Form eines zweiten Mobilfunkmoduls 2.1 der Datenzentrale 2 aus-
15 getauscht werden.

Das Fahrzeug 1 weist weiterhin eine mit dem ersten Mobilfunkmodul 1.1 verbundene erste Sicherheitseinrichtung in Form eines ersten Sicherheitsmoduls 1.2 auf. Spätestens wenn über das Mobilfunknetz 3 sicherheitsrelevante Daten von dem Fahrzeug 1 zur Datenzentrale 2 übertragen werden sollen, generiert das erste Sicherheitsmodul 1.2 einen ersten Daten dar-
20 stellenden ersten Datensatz, der unter anderem die zu übertragenden sicherheitsrelevanten Daten umfasst. Anschließend authentifiziert das erste Sicherheitsmodul 1.2 die ersten Daten unter Verwendung kryptographischer Mittel.

Hierzu ordnet das erste Sicherheitsmodul 1.2 dem ersten Datensatz eine Authentifizierungsinformation zu, indem es zunächst unter Verwendung eines entsprechenden kryptographischen Algorithmus und eines privaten ersten kryptographischen Schlüssels des Si-
25 cherheitsmoduls 1.2 über dem ersten Datensatz eine erste digitale Signatur als Authentifizierungsinformation bildet. Anschließend bildet das Sicherheitsmodul 1.2 aus dem ersten Datensatz und der ersten digitalen Signatur einen zweiten Datensatz.

Die erste digitale Signatur, also die Authentifizierungsinformation, stellt sicher, dass zu ei-
30 nem späteren Zeitpunkt durch eine Verifikation der ersten digitalen Signatur zweifelsfrei festgestellt werden kann, ob der erste Datensatz und damit die ersten Daten manipuliert wurden oder ob es sich nach wie vor um authentische Daten handelt.

Um die Sicherheit vor unbefugtem Zugriff auf die Daten zu erhöhen, verschlüsselt das erste Sicherheitsmodul 1.2 den zweiten Datensatz unter Verwendung eines zweiten kryptographischen Schlüssels, wobei ein dritter Datensatz entsteht. Dieser dritte Datensatz wird von dem ersten Sicherheitsmodul 1.2 an das erste Mobilfunkmodul 1.1 übergeben. Das erste Mobilfunkmodul 1.1 überträgt den dritten Datensatz dann über das Mobilfunknetz 3 an das zweite Mobilfunkmodul 2.1 der Datenzentrale 2.

Das zweite Mobilfunkmodul 2.1 gibt den dritten Datensatz an eine damit verbundene zweite Sicherheitseinrichtung in Form eines zweiten Sicherheitsmoduls 2.2 weiter. Das zweite Sicherheitsmodul 2.2 entschlüsselt den und dritten Datensatz unter Verwendung eines dritten kryptographischen Schlüssels, um so wieder den zweiten Datensatz zu erhalten. Der dritte Schlüssel entspricht dabei dem zweiten Schlüssel. Es handelt sich hierbei im vorliegenden Fall um einen zuvor ausschließlich für diese Übertragungssitzung generierten geheimen Sitzungsschlüssel. Dieser wurde zuvor separat in dem ersten Sicherheitsmodul 1.2 und dem zweiten Sicherheitsmodul 2.2 generiert. Die Generierung und Verwendung solcher geheimer einmalig verwendeter Sitzungsschlüssel ist an sich bekannt, sodass hierauf an dieser Stelle nicht näher eingegangen werden soll.

Es versteht sich jedoch, dass bei anderen Varianten der Erfindung, sofern eine solche Absicherung erforderlich ist, auch ein anderer Absicherungsmechanismus gewählt werden kann. Insbesondere kann bei Verwendung einer asymmetrischen Verschlüsselung der zweite kryptographische Schlüssel beispielsweise ein öffentlicher Schlüssel des zweiten Sicherheitsmoduls sein. Der dritte Schlüssel ist dann entsprechend der zugehörige private Schlüssel des zweiten Sicherheitsmoduls.

Aus dem zweiten Datensatz extrahiert das zweite Sicherheitsmodul 2.2 den ersten Datensatz und die erste digitale Signatur. Anhand des ersten Datensatzes und eines dem ersten kryptographischen Schlüssel zugeordneten vierten kryptographischen Schlüssels verifiziert das zweite Sicherheitsmodul 2.2 dann in an sich bekannter Weise die erste digitale Signatur, um die Authentizität des ersten Datensatzes und damit der ersten Daten festzustellen.

Derselbe Ablauf ergibt sich in der anderen Richtung, wenn sicherheitsrelevante Daten von der Datenzentrale 2 an das Fahrzeug 1 übermittelt werden sollen. Hierbei führt das zweite Sicherheitsmodul 2.2 dann die oben für das erste Sicherheitsmodul 1.2 beschriebenen Operationen durch und umgekehrt.

Im Rahmen der Kommunikation zwischen dem Fahrzeug 1 und der Datenzentrale 2 findet eine starke wechselseitige Authentifizierung der Kommunikationspartner unter Einsatz ent-

sprechender kryptographischer Mittel statt, wobei insbesondere entsprechende kryptographische Zertifikate Verwendung finden. Dies geschieht wiederum unter Verwendung des ersten Sicherheitsmoduls 1.2 und des zweiten Sicherheitsmoduls 2.2. Verfahren für eine solche starke wechselseitige Authentifizierung der Kommunikationspartner sind hinlänglich bekannt, sodass hierauf nicht näher eingegangen werden soll.

Figur 2 zeigt ein Blockschaltbild von Komponenten des Fahrzeugs 1. Wie dieser Figur zu entnehmen ist, weist das erste Sicherheitsmodul 1.2 eine erste Verarbeitungseinheit 1.3 auf, die mit dem ersten Mobilfunkmodul 1.1 verbunden ist. Mit der ersten Verarbeitungseinheit 1.3 ist weiterhin ein Kryptographiemodul 1.4 verbunden, welches die oben beschriebenen kryptographischen Mittel zur Verfügung stellt und hierzu entsprechende Kryptographiedaten enthält. Die Kryptographiedaten umfassen unter anderem kryptographischen Algorithmen und entsprechende kryptographische Schlüssel. Neben den kryptographischen Algorithmen und Schlüsseln umfassen die Kryptographiedaten des Kryptographiemoduls 1.4 weitere Daten, wie beispielsweise ein oder mehrere kryptographische Zertifikate entsprechender Zertifizierungsinstanzen sowie gegebenenfalls ein oder mehrere eigene kryptographische Zertifikate der Sicherheitseinrichtung 1.2.

Das Sicherheitsmodul 1.2 ist zum Austausch wenigstens eines Teils der Kryptographiedaten ausgebildet, um eine einfache und dauerhaft zuverlässige Sicherung der Daten zu gewährleisten. Hierbei ist vorgesehen, dass neben den kryptographischen Schlüsseln und kryptographischen Zertifikaten auch der jeweils verwendete kryptographische Algorithmus ausgetauscht werden kann, um das System an geänderte Sicherheitsanforderungen anpassen zu können. Die Implementierung und der Austausch der Kryptographiedaten erfolgt im Rahmen einer so genannten Public Key Infrastruktur (PKI), wie sie hinlänglich bekannt ist und daher an dieser Stelle nicht weiter beschrieben werden soll. Es versteht sich insbesondere, dass eine entsprechende Routine zur Überprüfung der Validität der verwendeten kryptographischen Zertifikate vorgesehen ist. Geeignete derartige Überprüfungsroutinen sind ebenfalls hinlänglich bekannt und sollen daher hier nicht näher beschrieben werden

Das Kryptographiemodul 1.4 wird sowohl zur Verschlüsselung zu speichernder Daten verwendet werden als auch zur Verschlüsselung zu übertragender Daten. Es versteht sich, dass je nach Anwendung, also beispielsweise je nachdem, ob Daten versandt oder gespeichert werden sollen, auch unterschiedliche kryptographische Verfahren angewendet werden können.

Nach der erfolgreichen Übertragung des dritten Datensatzes erstellt das erste Sicherheitsmodul 1.2 einen Protokolldatensatz, den es in einem mit der ersten Verarbeitungseinheit 1.3 verbundenen ersten Protokollspeicher 1.5 ablegt. Der Protokolldatensatz umfasst den ersten Datensatz sowie die über dem ersten Datensatz in der oben beschriebenen Weise erstellte erste digitale Signatur. Der umfasst mit anderen Worten also die authentifizierten ersten Daten. Der erste Protokollspeicher 1.5 kann dabei so gestaltet sein, dass der Protokolldatensatz lediglich gelesen aber nicht verändert werden kann. Weiterhin kann der erste Protokollspeicher 1.5 so dimensioniert sein, dass er sämtliche über die Lebensdauer des ersten Sicherheitsmoduls 1.2 oder des Fahrzeugs 1 zu erwartenden Protokolldatensätze aufnehmen kann.

Im vorliegenden Beispiel werden die Protokolldatensätze im Klartext gespeichert. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung vorgesehen sein kann, dass die Protokolldatensätze in verschlüsselter Form gespeichert werden können, um sie vor unbefugter Einsicht zu schützen.

Im Folgenden wird unter Bezugnahme auf die Figuren 1 und 2 die Generierung der an die Datenzentrale 2 zu übertragenden sicherheitsrelevanten ersten Daten näher beschrieben.

Die ersten Daten umfassen zum einen erste Erfassungswerte einer ersten Erfassungsgröße, die durch eine mit der ersten Verarbeitungseinheit 1.3 verbundene erste Erfassungseinrichtung 4 erfasst wurden. Bei den ersten Erfassungswerten handelt es sich um die aktuellen Werte des Kilometerstands des Fahrzeugs 1 als erster Erfassungsgröße. Diese Kilometerwerte werden von dem Kilometerzähler 4 des Fahrzeugs 1 als erster Erfassungseinrichtung erfasst und zu vorgegebenen Zeiten, beispielsweise in regelmäßigen Abständen, an die erste Verarbeitungseinheit 1.3 weitergegeben.

Die erste Verarbeitungseinheit 1.3 verknüpft diese Kilometerwerte mit einer für den Zeitpunkt ihrer Erfassung charakteristischen Erfassungszeitkennung, einem so genannten Zeitstempel, indem sie den Kilometerwert und die Erfassungszeitkennung in einen ersten Kilometerdatensatz schreibt. Hierzu greift sie auf ein Zeiterfassungsmodul 1.6 des ersten Sicherheitsmoduls 1.2 zu, welches eine entsprechend zuverlässige Zeitinformation liefert. Bei dem Zeiterfassungsmodul handelt es sich um eine integrierte Echtzeituhr, die von Zeit zu Zeit mit einer entsprechend genauen Zeitquelle synchronisiert wird. Es versteht sich, dass es sich bei anderen Varianten der Erfindung ebenso um ein Modul handeln kann, das über eine geeignete Kommunikationsverbindung zu einer entsprechenden Instanz die Echtzeit abfragt.

Die erste Verarbeitungseinheit 1.3 verknüpft die Kilometerwerte weiterhin mit einer für den Kilometerzähler 4 charakteristischen ersten Erfassungseinrichtungskennung, indem sie diese ebenfalls in den ersten Kilometerdatensatz schreibt. Hierbei handelt es sich um eine für den betreffenden Kilometerzähler 4 einmalige und eindeutige Identifikation, die gleichzeitig eine erste Quellenidentifikation für die Quelle der Kilometerwerte darstellt. Die erste Erfassungseinrichtungskennung stellt gleichzeitig eine erste Erfassungsgrößenkennung dar, da der Kilometerzähler 4 ausschließlich Kilometerwerte liefert. Es versteht sich, dass bei anderen Erfassungseinrichtungen, die unterschiedliche Erfassungsgrößen erfassen, den jeweiligen Erfassungswerten gegebenenfalls mit einer entsprechenden Erfassungsgrößenkennung verknüpft werden können.

Es versteht sich, dass die vorgenannte Verknüpfung der Kilometerwerte mit der Erfassungszeitkennung und der Erfassungseinrichtungskennung durch kryptographische Mittel abgesichert werden kann. So kann beispielsweise vorgesehen sein, dass das erste Sicherheitsmodul 1.2 eine zweite digitale Signatur über diesen Daten erstellt, sodass diese durch die ihnen dann beigefügte zweite digitale Signatur ebenfalls manipulationssichere miteinander verknüpft sind. Ebenso kann natürlich für beliebige andere einander zugeordnete Daten verfahren werden, um diese manipulationssicher miteinander zu verknüpfen.

Der so generierte erste Kilometerdatensatz wird dann von der ersten Verarbeitungseinheit 1.3 in einem mit ihr verbundenen ersten Speicher 1.7 abgelegt.

Die ersten Daten umfassen weiterhin zweite Erfassungswerte einer zweiten Erfassungsgröße und dritte Erfassungswerte einer dritten Erfassungsgröße, die durch eine mit der ersten Verarbeitungseinheit 1.3 verbundene zweite Erfassungseinrichtung 5 erfasst wurden. Bei den zweiten Erfassungswerten handelt es sich um die aktuellen Werte des Motorölstands des Fahrzeugs 1 als zweiter Erfassungsgröße. Bei dritten Erfassungswerten handelt es sich um die aktuellen Werte der Bremsenqualität des Fahrzeugs 1 als dritter Erfassungsgröße. Diese Bremsenqualitätswerte werden von der Fahrzeugüberwachungseinrichtung 5 des Fahrzeugs 1 als zweiter Erfassungseinrichtung erfasst und ebenfalls zu vorgegebenen Zeiten, beispielsweise in regelmäßigen Abständen, an die erste Verarbeitungseinheit 1.3 weitergegeben.

Die erste Verarbeitungseinheit 1.3 verknüpft diese zweiten und dritten Erfassungswerte mit einer für den Zeitpunkt ihrer Erfassung charakteristischen Erfassungszeitkennung, indem sie den Motorölstandswert, den Bremsenqualitätswert und die Erfassungszeitkennung in einen

ersten Fahrzeugzustandsdatensatz schreibt. Hierzu greift sie auf ein Zeiterfassungsmodul 1.6 der ersten Sicherheitseinrichtung 1.2 zu.

Die erste Verarbeitungseinheit 1.3 verknüpft die Motorölstandswerte und die Bremsenqualitätswerte weiterhin mit einer für die Fahrzeugüberwachungseinrichtung 5 charakteristischen zweiten Erfassungseinrichtungskennung, indem sie diese ebenfalls in den ersten Fahrzeugzustandsdatensatz schreibt. Hierbei handelt es sich um eine für die betreffende Fahrzeugüberwachungseinrichtung 5 einmalige und eindeutige Identifikation, die gleichzeitig eine zweite Quellenidentifikation für die Quelle der Motorölstandswerte und Bremsenqualitätswerte darstellt. Weiterhin wird den jeweiligen Erfassungswerten eine entsprechenden Erfassungsgrößenkennung zugeordnet, indem diese entsprechend zugeordnet mit in den Fahrzeugzustandsdatensatz geschrieben wird.

Der so generierte erste Fahrzeugzustandsdatensatz wird dann von der ersten Verarbeitungseinheit 1.3 ebenfalls in dem ersten Speicher 1.7 abgelegt.

Zu einem bestimmten vorgegebenen oder wählbaren Zeitpunkt sollen dann die zwischenzeitlich im ersten Speicher 1.7 abgelegten Kilometerdatensätze und Fahrzeugzustandsdatensätze als erste Überwachungsdaten an die Datenzentrale 2 übertragen werden. Die erste Verarbeitungseinheit 1.3 liest hierzu die gespeicherten Kilometerdatensätze und Fahrzeugzustandsdatensätze aus dem ersten Speicher 1.7 aus und schreibt sie in den ersten Datensatz.

Die erste Verarbeitungseinheit 1.3 ergänzt den ersten Datensatz weiterhin um eine dem ersten Sicherheitsmodul 1.2 zugeordnete einmalige und eindeutige erste Sicherheitsmodulidentifikation sowie um einen unter Zugriff auf das erste Zeiterfassungsmodul 1.6 generierten ersten Zeitstempel. Die erste Sicherheitsmodulidentifikation stellt dabei eine dritte Quellenidentifikation dar, während der erste Zeitstempel den Zeitpunkt der Zusammenstellung der ersten Überwachungsdaten charakterisiert. Weiterhin ergänzt die erste Verarbeitungseinheit 1.3 den ersten Datensatz um eine einmalige und eindeutige Identifikation des ersten Mobilfunkmoduls 1.1, die ebenfalls als Quellenidentifikation dient.

Schließlich ergänzt die erste Verarbeitung einer 1.3 den ersten Datensatz um eine Übertragungsidentifikation in Form einer fortlaufenden Transaktionsnummer, die dem laufenden Übertragungsvorgang eindeutig zugeordnet ist.

Anschließend wird der erste Datensatz in der oben beschriebenen Weise authentifiziert und in Form des dritten Datensatzes an die Datenzentrale 2 übertragen.

Sobald die Datenzentrale 2 die Authentizität des ersten Datensatzes überprüft hat, sendet sie einen entsprechenden Bestätigungsdatensatz an das Fahrzeug 1. Dieser Bestätigungsdatensatz umfasst eine dem zweiten Sicherheitsmodul zugeordnete zweiten Sicherheitsmodulidentifikation. Die zweite Sicherheitsmodulidentifikation stellt dabei eine erste Empfängeridentifikation dar, die den Empfänger des ersten Datensatzes kennzeichnet.

Die erste Verarbeitungseinheit 1.3 schreibt diesen Bestätigungsdatensatz zusammen mit einem für den Zeitpunkt des Erhalts des Bestätigungsdatensatzes charakteristischen zweiten Zeitstempel in den vorhandenen ersten Datensatz und authentifiziert diesen dann wieder in der oben beschriebenen Weise, indem sie eine digitale Signatur über dem ersten Datensatz bildet. Diese digitale Signatur wird dann zusammen mit dem ersten Datensatzes in einen ersten Protokolldatensatz geschrieben, der dann in der oben beschriebenen Weise in den ersten Protokollspeicher 1.5 eingebracht wird.

Der erste Protokolldatensatz wird anschließend an die Datenzentrale 2 übermittelt, wo er nach entsprechender Überprüfung seiner Authentizität in einem mit dem zweiten Sicherheitsmodul 2.2 verbundenen zweiten Protokollspeicher 2.3 gespeichert wird. Es versteht sich, dass die Datenzentrale 2 bei anderen Varianten der Erfindung auch einen solchen Protokolldatensatz selbst generieren und in den zweiten Protokollspeicher ablegen kann.

Dieser erste Protokolldatensatz authentifiziert somit in vorteilhafter Weise sowohl die Quellen und den Empfänger der jeweiligen Daten, bestimmte Erfassungs- und Verarbeitungszeitpunkte sowie die Übertragung selbst, sodass die mit diesen Daten verbundenen Sachverhalte zu einem späteren Zeitpunkt zweifelsfrei nachgewiesen werden können. Insbesondere ist es möglich, den Empfang der ersten Daten in der Datenzentrale 2 nachzuweisen.

Nach Erhalt und Überprüfung der Authentizität der ersten Daten in der Datenzentrale 2 werden diese alleine mit dem Sicherheitsmodul 2.2 verbundene Analyseeinrichtung 2.4 der Datenzentrale 2 übermittelt. Diese analysiert die übermittelten ersten Daten. Hierbei berücksichtigt die unter anderem statistische Daten, welche nicht von dem Fahrzeug 1 stammen.

Die Analyseeinrichtung 2.4 löst zum einen in Abhängigkeit von den übermittelten Kilometerwerten als erste Überwachungsreaktion einen ersten Abrechnungsvorgang für die gefahrenen Kilometer durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene Abrechnungsmodul 2.5 als erster Überwachungsreaktionseinrichtung aus.

Als zweite Überwachungsreaktion löst die Analyseeinrichtung 2.4 in Abhängigkeit von der Analyse der ersten Daten die Generierung von Betriebsbeeinflussungsdaten für das Fahr-

zeug 1 durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene zweite Überwachungsreaktionseinrichtung 2.6 aus. Diese Betriebsbeeinflussungsdaten werden in einem weiteren ersten Datensatz von der Datenzentrale 2 über das Mobilfunknetz 3 an das Fahrzeug 1 übermittelt. Hierbei wird analog zu der oben beschriebenen Übermittlung der ersten Daten von dem Fahrzeug 1 zu Datenzentrale 2 verfahren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird. Insbesondere werden die ersten Daten in analoger Weise authentifiziert und es wird ein entsprechender Protokolldatensatz für die Übertragung generiert und sowohl im Fahrzeug 1 als auch in der Datenzentrale 2 gespeichert.

Die Betriebsbeeinflussungsdaten umfassen zum einen in Abhängigkeit von den übermittelten Kilometerwerten einen Hinweis über die aktuell gefahrenen Kilometer, den hierfür aktuellen Tarif sowie den aktuellen Abrechnungswert. Dieser Hinweis wird nach Verifizierung der Authentizität der Betriebsbeeinflussungsdaten im ersten Sicherheitsmodul 1.2 an eine mit dem ersten Sicherheitsmodul 1.2 verbundene Betriebsbeeinflussungseinrichtung 6 weitergegeben, welche diesen wiederum über ein damit verbundenes Display 7 an den Nutzer des Fahrzeugs 1 ausgibt. Die Betriebsbeeinflussungsdaten können weiterhin in Abhängigkeit von der Analyse der übermittelten Fahrzeugüberwachungsdaten (Motorölstand und Bremsenqualität) im Falle des Drohens kritischer Zustände entsprechende Warnhinweise enthalten, die ebenfalls über das Display 7 an den Nutzer des Fahrzeugs 1 ausgegeben werden.

Schließlich löst die Analyseeinrichtung 2.4 als dritte Überwachungsreaktion in Abhängigkeit von der Analyse der ersten Daten die Durchführung eines Wartungsprotokolls für das Fahrzeug 1 durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene dritte Überwachungsreaktionseinrichtung in Form einer Fahrzeugmanagementeinrichtung 2.7 aus. Hierbei kann in Abhängigkeit von den Überwachungsdaten unter anderem die Wartung des Fahrzeuges 1 bei Rückgabe geplant und vorbereitet werden. Insbesondere können erforderliche Ersatzteile oder dergleichen bereits vorab bestellt werden, um die erforderliche Zeit für die Wartung so kurz wie möglich zu halten und damit die Ausfallzeiten des Fahrzeugs 1 zu verringern.

Die Erfassungseinrichtungen 4 und 5, das erste Sicherheitsmodul 1.2 und das erste Mobilfunkmodul 1.1 sind in einer vor unbefugtem Zugriff geschützten sicheren Umgebung 1.3 angeordnet, um den unbefugten Zugriff nicht nur auf die Daten des Sicherheitsmoduls ein vom zweiten sondern auch auf die Daten, die von und zu den Erfassungseinrichtungen 4 und 5 bzw. dem ersten Mobilfunkmodul 1.1 geliefert werden, wirksam zu unterbinden.

Die sichere Umgebung 1.3 wird zum einen physisch durch sichere Gehäuse der Erfassungseinrichtungen 4 und 5, des Mobilfunkmoduls 1.1 und des ersten Sicherheitsmoduls 1.2 hergestellt, die mit hinlänglich bekannten Mitteln zur Erfassung von Manipulationen am Gehäuse ausgestattet sind. Zum anderen wird sie logisch durch ein entsprechend abgesichertes Kommunikationsprotokoll zwischen diesen Komponenten hergestellt. So wird bei jeder Kommunikation zwischen diesen Komponenten über eine entsprechend starke gegenseitige Authentifizierung ein gesicherter Kommunikationskanal aufgebaut. Es versteht sich, dass die Komponenten hierzu über entsprechende Kommunikationsmittel verfügen, welche die beschriebenen Sicherheitsfunktionalitäten zur Verfügung stellen.

Es versteht sich jedoch, dass bei anderen Varianten der Erfindung je nach den zu stellenden Sicherheitsanforderungen keine oder lediglich einzelne der genannten Komponenten in einer entsprechenden sicheren Umgebung angeordnet sein können.

Figur 3 zeigt ein weiteres bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung, die in ihrer grundsätzlichen Funktion derjenigen aus Figur 1 gleicht, sodass hier lediglich auf die Unterschiede eingegangen werden soll.

Ein Unterschied besteht darin, dass es sich bei der mit dem ersten Sicherheitsmodul 1.2' verbundenen ersten Übertragungseinrichtung des Fahrzeugs 1' um eine kurzreichweitige erste Infrarotschnittstelle 1.1' handelt. Die Infrarotschnittstelle 1.1' arbeitet dabei nach dem IrDA-Standard. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung auch beliebige andere Übertragungsverfahren mit kurzer Reichweite, wie beispielsweise Bluetooth etc., verwendet werden können.

Die zweite Übertragungseinrichtung ist von einem Serviceterminal 8 gebildet. Dieses Serviceterminal 8 umfasst eine entsprechende zweite Infrarotschnittstelle 8.1 und ein damit verbundenes Kommunikationsmodul 8.2, welches die von der zweiten Infrarotschnittstelle 8.1 empfangenen ersten Daten über ein Telekommunikationsnetz 9 an die Datenzentrale 2' übermittelt.

Die Generierung, Authentifizierung, Übermittlung und Protokollierung der sicherheitsrelevanten ersten Daten von dem Fahrzeug 1' zur Datenzentrale 2' und umgekehrt erfolgt analog der oben in Zusammenhang mit Figur 1 beschriebenen Ausführungsform, sodass hier lediglich auf die obigen Ausführungen verwiesen wird.

Ein weiterer Unterschied besteht darin, dass das erste Sicherheitsmodul 1.2' mit einer Fahrzeugmanagementüberwachungseinrichtung 10 verbunden ist, die wiederum mit der Fahr-

zeugmanagementeinrichtung 11 des Fahrzeugs 1' verbunden ist. Die Fahrzeugmanagementeinrichtung 11 stellt dabei diejenige Einrichtung dar, welche die Funktionen der einzelnen Komponenten des Fahrzeugs steuert. Sie umfasst insbesondere das Motormanagement etc.

- 5 Die Fahrzeugmanagementüberwachungseinrichtung 10 überwacht in diesem Fall als dritte Erfassungseinrichtung unter anderem die Funktion der Softwarekomponenten der Fahrzeugmanagementeinrichtung 11. Die von der Fahrzeugmanagementüberwachungseinrichtung 10 erfassten Daten werden als dritte Erfassungswerte und damit als Überwachungsdaten in der oben beschriebenen Weise in einen ersten Datensatz eingebracht, authentifiziert und an die Datenzentrale 2' übermittelt.

In Abhängigkeit von der Analyse der übermittelten Überwachungsdaten in der Datenzentrale 2' generiert, authentifiziert und sendet die Datenzentrale 2' entsprechende Betriebsbeeinflussungsdaten in der oben beschriebenen Weise über das Serviceterminal 8 an das Fahrzeug 1'. Bei der Analyse der Überwachungsdaten überprüft die Datenzentrale 2' nicht nur die
15 Integrität der Fahrzeugmanagementeinrichtung 11. Sie überprüft unter anderem auch die aktuelle Version der durch die Fahrzeugmanagementeinrichtung 11 verwendeten Softwaremodule. Existiert für eines der Softwaremodule eine neue Version, wird diese als Bestandteil der Betriebsbeeinflussungsdaten an das Fahrzeug 1' übersandt.

Nach dem das erste Sicherheitsmodul 1.2' die Authentizität der Betriebsbeeinflussungsdaten
20 in der oben beschriebenen Weise verifiziert hat, gibt es die Betriebsbeeinflussungsdaten, insbesondere das neue Softwaremodul an die Fahrzeugmanagementüberwachungseinrichtung 10 weiter. Diese Fahrzeugmanagementüberwachungseinrichtung 10 stellt gleichzeitig eine Betriebsbeeinflussungseinrichtung dar, indem sie den Austausch des nichtmehr aktuellen alten Softwaremoduls durch das neue Softwaremodul in der Fahrzeugmanagementeinrichtung 11 steuert.

Auch die Übertragung der Betriebsbeeinflussungsdaten von der Datenzentrale 2' zum Fahrzeug 1 wird in der oben beschriebenen Weise protokolliert. Hierbei wird in den entsprechenden ersten Datensatz zudem eine Identifikation des Serviceterminals 8 als Quellenidentifikation aufgenommen, um auch die Übertragung über dieses Serviceterminal 8 zu einem späteren zweifelsfrei nachvollziehen zu können.

Insbesondere wird hier die Identifikation des ersten Sicherheitsmoduls 1.2' als Empfängeridentifikation in den ersten Datensatz des Protokolldatensatzes aufgenommen. Dies kann in Fällen, in denen der Austausch des betreffenden Softwaremoduls kostenpflichtig ist, später

als Nachweis dienen, dass der Softwaremodul tatsächlich im Fahrzeug 1' empfangen wurde. Gegebenenfalls kann auch eine entsprechende Austauschbetätigung in den ersten Datensatz aufgenommen werden, um auch den tatsächlichen Austausch zweifelsfrei nachvollziehbar zu machen.

- 5 Es versteht sich, dass in solchen Fällen einer kostenpflichtigen Wartung der Fahrzeugsoftware oder auch bei anderen kostenpflichtigen Betriebsbeeinflussungen in der Datenzentrale mit Erhalt einer entsprechenden Empfangsbestätigung vom Fahrzeug 1' ein entsprechender Abrechnungsvorgang ausgelöst werden kann.

- 10 Die Kommunikation zwischen dem Fahrzeug 1' und der Datenzentrale 2' läuft wie die oben im Zusammenhang mit Figur 1 beschriebene Kommunikation ab. Insbesondere findet jeweils eine starke wechselseitige Authentifizierung unter Verwendung kryptographischer Mittel statt, sodass in Verbindung mit der Authentifizierung der ersten Daten jeweils gewährleistet ist, dass nur autorisierte und authentische Daten ausgetauscht und verwendet werden.

- 15 Mit dem beschriebenen Ausführungsbeispiel lässt sich beispielsweise ein flächendeckendes Netz von Serviceterminals 8 realisieren, über das eine einfache Überwachung und Fernwartung von Fahrzeugen möglich ist.

- 20 Das Ausführungsbeispiel wurde vorstehend anhand einer drahtlosen Verbindung zum Serviceterminal 8 beschrieben. Es versteht sich jedoch, dass bei anderen Varianten auch eine drahtgebundene Verbindung zum Serviceterminal vorgesehen sein kann, wie dies in Figur 3 durch den Pfeil 12 angedeutet ist. So kann beispielsweise ein Datenkabel verwendet werden, welches das Fahrzeug über entsprechende serielle Schnittstellen mit der zweiten Übertragungseinrichtung des Serviceterminals verbindet.

- 25 Weiterhin versteht es sich, dass es sich bei anderen Varianten der Erfindung bei dem Serviceterminal ebenfalls um eine mobile Einrichtung handeln kann, die dann gegebenenfalls über ein Mobilfunknetz oder dergleichen eine Verbindung zur Datenzentrale herstellt. Eine derartige Variante der Erfindung eignet sich besonders für den Einsatz in Zusammenhang mit Pannendiensten oder dergleichen.

- 30 Schließlich versteht es sich, dass das erste Sicherheitsmodul nicht notwendigerweise Bestandteil der mobilen Einheit sein muss. So ist es im Zusammenhang mit den soeben genannten Serviceterminals, insbesondere den mobilen Serviceterminals, möglich, das erste Sicherheitsmodul oder Teile davon, beispielsweise das Kryptographiemodul, in dem Serviceterminal zu integrieren. Dabei kann dann vorgesehen sein, dass die mobile Einrichtung

beispielsweise neben den Erfassungseinrichtungen sowie einer entsprechenden Schnittstelle zur Verbindung mit dem Serviceterminal lediglich den ersten Protokollspeicher aufweist, in den der Protokolldatensatz durch das Serviceterminal geschrieben wird.

Figur 4 zeigt ein weiteres bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung, die in ihrer grundsätzlichen Funktion derjenigen aus Figur 1 gleicht, sodass hier lediglich auf die Unterschiede eingegangen werden soll.

Ein Unterschied besteht darin, dass das erste Sicherheitsmodul 1.2" eines Lastkraftwagens als erstem Fahrzeug 1" über einen Fahrzeugdatenbus 13 nicht nur mit einer Erfassungseinrichtung 14 des Fahrzeugs 1" verbunden ist, über die Zustandsdaten des Fahrzeugs, unter anderem dessen Position, ermittelt werden. Vielmehr ist das erste Sicherheitsmodul 1.2" auch mit einer Erfassungseinrichtung 15.1 eines geladenen ersten Containers 15 und einer Erfassungseinrichtung 16.1 eines geladenen zweiten Containers 16 verbunden. Über die Erfassungseinrichtungen 15.1 und 16.1 werden jeweils Zustandsdaten des Containers 15 bzw. 16 und seiner Ladung erfasst.

Bei dem Fahrzeugdatenbus 13 handelt es sich im vorliegenden Fall um einen drahtlosen Datenbus. Es versteht sich jedoch, dass bei anderen Varianten der vorliegenden Erfindung auch ein drahtgebundener Datenbus verwendet werden kann.

Die Erfassungswerte der Erfassungseinrichtungen 14, 15.1 und 16.1 werden an das erste Sicherheitsmodul 1.2" weitergegeben und dann in der oben in Zusammenhang mit Figur 1 beschriebenen Weise über ein mit dem ersten Sicherheitsmodul 1.2" verbundenes erstes Mobilfunkmodul an eine - nicht dargestellte - entfernte Datenzentrale übermittelt.

Hiermit ist es nicht nur möglich, den Zustand des Fahrzeugs 1" zu überwachen und gegebenenfalls zu beeinflussen. Vielmehr ist es mit einem einzigen Sicherheitsmodul 1.2" auch möglich, den Zustand der Ladung des Fahrzeugs 1" zu überwachen und gegebenenfalls zu beeinflussen. Handelt es sich beispielsweise bei dem Container 15 um einen Kühlcontainer und wird über die Erfassungseinrichtung ein Anstieg der Temperatur im Container 15 über einen vorgegebenen Grenzwert ermittelt, so kann in der oben beschriebenen Weise über die Datenzentrale eine Betriebsbeeinflussung erfolgen. Hierzu kann beispielsweise durch entsprechende von der Datenzentrale übermittelte Betriebsbeeinflussungsdaten die Kühlleistung des Kühlaggregats 15.2 des Containers 15 erhöht werden. Zudem kann durch die gespeicherten und in der oben beschriebenen Weise authentifizierten Protokolldatensätze gegebenenfalls zweifelsfrei der Temperaturverlauf im Inneren des Containers 15 nachgewiesen werden. Dies kann beispielsweise beim Transport von verderblichen Lebensmitteln,

wie Fleisch oder dergleichen, dazu verwendet werden, nachzuweisen, dass die Temperatur der Lebensmittel für die Zeit, die sie im Inneren des Containers 15 aufbewahrt wurden, stets unterhalb vorgeschriebener Grenzwerte lag.

5 Weiterhin ist es durch die Ermittlung der Position des Fahrzeugs 1" durch die Erfassungseinrichtung 14 insbesondere möglich, den Standort der Container 15 und 16 nachzuvollziehen. Insbesondere können diese Erkenntnisse in eine übergeordnete Logistikplanung einfließen.

Die Positionsbestimmung durch die Erfassungseinrichtung 14 kann in beliebiger bekannter Weise erfolgen. So kann die Erfassungseinrichtung 14 ein entsprechendes GPS-Modul.
10 Ebenso kann aber auch in bekannter Weise eine Positionsbestimmung über das Mobilfunknetz 3" erfolgen.

Auch hier sei erwähnt, dass die Kommunikation zwischen dem Fahrzeug 1" und der Datenzentrale wie die oben im Zusammenhang mit Figur 1 beschriebene Kommunikation abläuft. Insbesondere findet jeweils eine starke wechselseitige Authentifizierung unter Verwendung
15 kryptographischer Mittel statt; sodass in Verbindung mit der Authentifizierung der ersten Daten jeweils gewährleistet ist, dass nur autorisierte und authentische Daten ausgetauscht und verwendet werden.

Die vorliegende Erfindung wurde vorstehend ausschließlich anhand von Beispielen für Fahrzeuge beschrieben. Es versteht sich jedoch, dass Erfindung auch im Zusammenhang mit
20 beliebigen anderen beweglichen Einrichtungen, wie beispielsweise Containern etc. zur Anwendung kommen kann.

* * * * *

Patentansprüche

1. Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1''), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') erfolgt, dadurch gekennzeichnet, dass die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung einer ersten Quelle (1.2, 4, 5; 8) der ersten Daten eine erste Quellenidentifikation umfassen.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung eines ersten Empfängers (2.2) der ersten Daten eine erste Empfängeridentifikation umfassen.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung der Übertragung der ersten Daten eine Übertragungsidentifikation umfassen.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten wenigstens eine für ein vorgebbares Ereignis charakteristische Zeitkennung umfassen.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die authentifizierten ersten Daten in einen Protokolldatensatz eingefügt werden, der in der ersten Einrichtung (1; 1'; 1'') und/oder der Datenzentrale (2; 2') gespeichert wird.
7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten unter Verwendung wenigstens einer ersten digitalen Signatur authentifiziert werden.
8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Er-

fassungswert einer ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) der ersten Einrichtung (1; 1'; 1'') erfasst wurde.

- 5 9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass die erste Erfassungsgröße eine Zustandsgröße der ersten Einrichtung (1; 1'; 1'') ist.
10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten wenigstens Betriebsbeeinflussungsdaten umfassen, die zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'') an die erste Einrichtung (1; 1'; 1'') übermittelt werden.
- 10 11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Daten über wenigstens eine zweite Datenübertragungseinrichtung (3.1; 8.2) übertragen werden.
- 15 12. Verfahren zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, bei dem zwischen der mobilen ersten Einrichtung (1; 1'; 1'') und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2') über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') erste Daten mit einem Verfahren nach einem der vorhergehenden Ansprüche übertragen werden, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, wobei
- 20
- die ersten Überwachungsdaten wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) der ersten Einrichtung erfasst wurde,
 - die ersten Überwachungsdaten in der Datenzentrale (2; 2') verifiziert werden und
 - 25 - die ersten Überwachungsdaten bei erfolgreicher Verifikation in der Datenzentrale (2; 2') analysiert werden.
13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass in der Datenzentrale (2; 2') in Abhängigkeit von der Analyse der ersten Überwachungsdaten eine erste Überwachungsreaktion ausgelöst wird.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die erste Überwachungsreaktion einen Abrechnungsvorgang umfasst.
15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die erste Überwachungsreaktion die Generierung von Betriebsbeeinflussungsdaten umfasst, die zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'') an die erste Einrichtung (1; 1'; 1'') übermittelt werden.
16. Verfahren nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, dass bei der Analyse weitere, nicht von der ersten Einrichtung (1; 1'; 1'') übermittelte Daten berücksichtigt werden.
17. Anordnung zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei zur Übertragung der Daten wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') vorgesehen ist, dadurch gekennzeichnet, dass die übertragenen Daten erste Daten umfassen und wenigstens eine Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') vorgesehen ist, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.
18. Anordnung nach Anspruch 17, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zur Authentifizierung einer ersten Quelle (1.2, 4, 5; 8) der ersten Daten zum Einbringen einer ersten Quellenidentifikation in den ersten Datensatz ausgebildet ist.
19. Anordnung nach Anspruch 17 oder 18, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zur Authentifizierung eines ersten Empfängers (2.2) der ersten Daten zum Einbringen einer ersten Empfängeridentifikation in den ersten Datensatz ausgebildet ist.
20. Anordnung nach einem der Ansprüche 17 bis 19, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2; 1.2'; 1.2'') zur Authentifizierung der Übertragung der ersten Daten zum Einbringen einer Übertragungsidentifikation in den ersten Datensatz ausgebildet ist.
21. Anordnung nach einem der Ansprüche 17 bis 20, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zum Einbringen wenigstens einer für ein

vorgebbares Ereignis charakteristischen Zeitkennung in den ersten Datensatz ausgebildet ist.

- 5 22. Anordnung nach einem der Ansprüche 17 bis 21, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zum Einbringen der authentifizierten ersten Daten in einen Protokolldatensatz ausgebildet ist und dass die erste Einrichtung (1; 1'; 1'') einen ersten Protokollspeicher (1.5) zum Speichern des Protokolldatensatzes aufweist und/oder die Datenzentrale (2; 2') einen zweiten Protokollspeicher (2.3) zum Speichern des Protokolldatensatzes aufweist.
- 10 23. Anordnung nach einem der Ansprüche 17 bis 22, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zur Bildung einer ersten digitalen Signatur unter Verwendung der ersten Daten ausgebildet ist.
24. Anordnung nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass die erste Einrichtung (1; 1'; 1'') eine erste Sicherheitseinrichtung (1.2; 1.2'; 1.2'') umfasst und/oder die Datenzentrale (2; 2') eine zweite Sicherheitseinrichtung (2.2) umfasst.
- 15 25. Anordnung nach einem der Ansprüche 17 bis 24, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, wobei die erste Einrichtung eine erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung des ersten Erfassungswerts umfasst.
- 20 26. Anordnung nach Anspruch 25, dadurch gekennzeichnet, dass die erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung einer Zustandsgröße der ersten Einrichtung (1; 1'; 1'') als erster Erfassungsgröße ausgebildet ist.
- 25 27. Anordnung nach einem der Ansprüche 17 bis 26, dadurch gekennzeichnet, dass die ersten Daten von der Datenzentrale (2; 2') zur ersten Einrichtung (1; 1'; 1'') übertragene Betriebsbeeinflussungsdaten umfassen, wobei die erste Einrichtung (1; 1'; 1'') eine Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'', 15) in Abhängigkeit von den Betriebsbeeinflussungsdaten aufweist.

28. Anordnung nach einem der Ansprüche 17 bis 27, dadurch gekennzeichnet, dass zur Datenübertragung zwischen der ersten Einrichtung (1; 1') und der Datenzentrale (2; 2') wenigstens eine zweite Datenübertragungseinrichtung (3.1; 8.2) vorgesehen ist.

5 29. Anordnung zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, mit einer Anordnung zur Übertragung von ersten Daten nach einem der Ansprüche 17 bis 28, dadurch gekennzeichnet, dass

- die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale übertragene (2; 2') erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, wobei die erste Einrichtung (1; 1'; 1'') eine erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung des ersten Erfassungswerts umfasst,
- die Datenzentrale (2; 2') eine zweite Sicherheitseinrichtung (2.2) zum Verifizieren der ersten Überwachungsdaten aufweist und
- die Datenzentrale (2; 2') eine mit der zweiten Sicherheitseinrichtung (2.2) verbundene Analyseeinrichtung (2.4) zum Analysieren der ersten Überwachungsdaten in Abhängigkeit vom Ergebnis der Verifikation aufweist.

10 30. Anordnung nach Anspruch 29, dadurch gekennzeichnet, dass wenigstens eine mit der Analyseeinrichtung (2.4) verbindbare Überwachungsreaktionseinrichtung (2.5, 2.6, 2.7) zur Durchführung einer ersten Überwachungsreaktion vorgesehen ist und die Analyseeinrichtung (2.4) zum Ansteuern der Überwachungsreaktionseinrichtung (2.5, 2.6, 2.7) zum Auslösen einer ersten Überwachungsreaktion in Abhängigkeit vom Ergebnis der Analyse der ersten Überwachungsdaten ausgebildet ist.

20 31. Anordnung nach Anspruch 30, dadurch gekennzeichnet, dass als Überwachungsreaktionseinrichtung eine mit der Analyseeinrichtung (2.4) verbindbare Abrechnungseinrichtung (2.5) vorgesehen ist.

25 32. Anordnung nach Anspruch 30 oder 31, dadurch gekennzeichnet, dass

- die Überwachungsreaktionseinrichtung (2.6, 2.7) zur Generierung von Betriebsbeeinflussungsdaten zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'', 15) als erste Überwachungsreaktion ausgebildet ist,

- die Datenzentrale (2; 2') zur Übertragung erster Daten an die erste Einrichtung (1; 1'; 1'') ausgebildet ist, wobei die ersten Daten die Betriebsbeeinflussungsdaten umfassen, und
- die erste Einrichtung (1; 1'; 1'') eine Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten aufweist.

33. Anordnung nach Anspruch 32, dadurch gekennzeichnet, dass

- die erste Einrichtung (1; 1'; 1'') eine erste Sicherheitseinrichtung (1.2; 1.2'; 1.2'') umfasst, die zum Verifizieren der die Betriebsbeeinflussungsdaten umfassenden ersten Daten ausgebildet ist und
- die Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'', 15) in Abhängigkeit vom Ergebnis der Verifizierung ausgebildet ist.

34. Anordnung nach einem der Ansprüche 29 bis 33, dadurch gekennzeichnet, dass die Analyseeinrichtung (2.4) zur Berücksichtigung weiterer, nicht von der ersten Einrichtung übermittelter Daten ausgebildet ist.

35. Mobile erste Einrichtung, insbesondere Fahrzeug, für eine Anordnung nach einem der Ansprüche 17 bis 34, gekennzeichnet durch eine erste Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') zur Übertragung erster Daten und eine mit der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') verbindbare erste Sicherheitseinrichtung (1.2; 1.2'; 1.2''), die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

36. Mobile erste Einrichtung nach Anspruch 35, dadurch gekennzeichnet, dass die erste Sicherheitseinrichtung (1.2; 1.2'; 1.2'') zur Authentifizierung der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') zum Einbringen einer der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') zugeordneten Identifikation in den ersten Datensatz ausgebildet ist.

37. Datenzentrale für eine Anordnung nach einem der Ansprüche 17 bis 34, gekennzeichnet durch eine Datenübertragungseinrichtung (2.1) zur Übertragung erster Da-

ten und eine mit der Datenübertragungseinrichtung (2.1) verbindbare zweite Sicherheitseinrichtung (2.2), die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

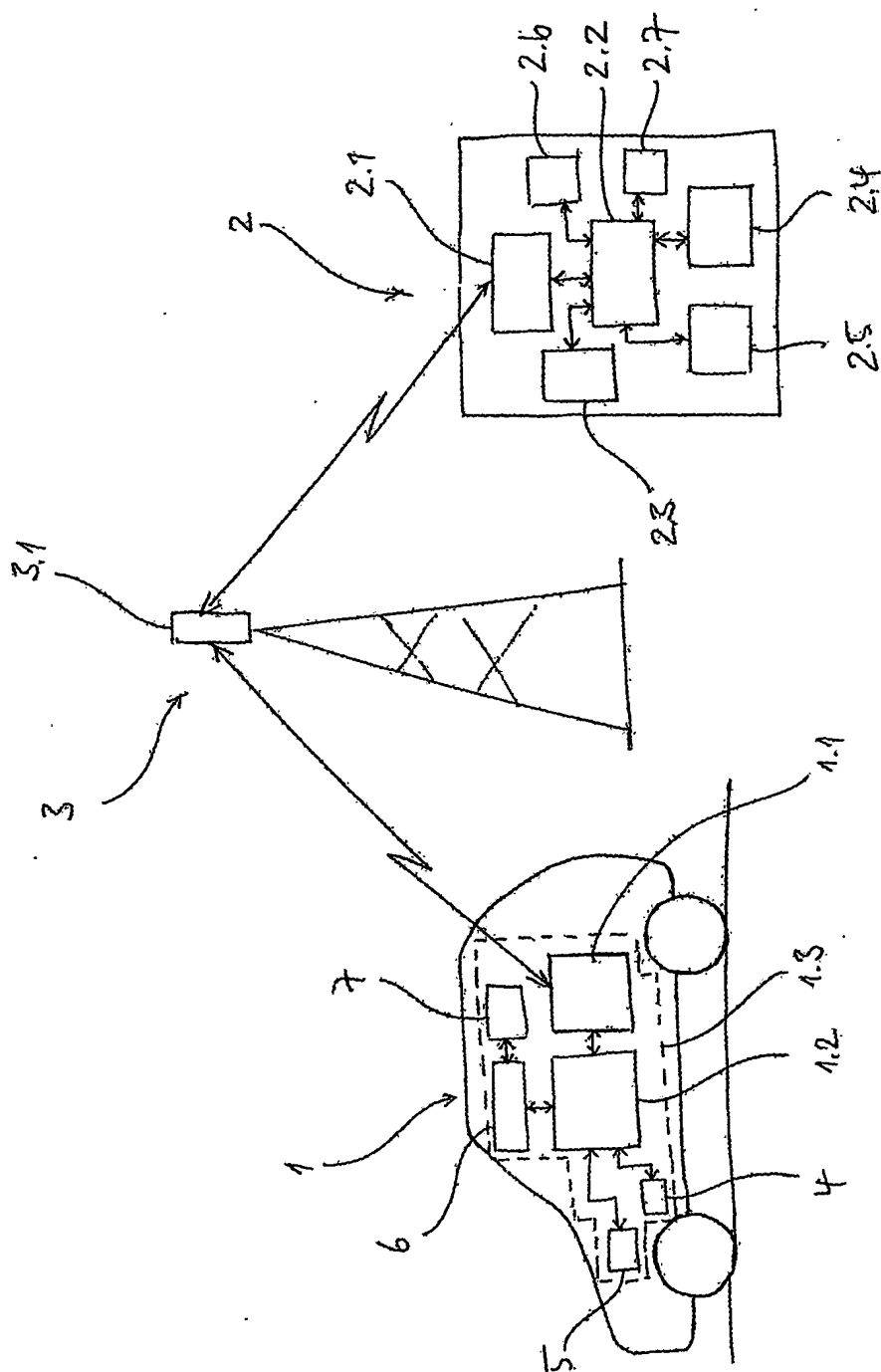


Fig. 1

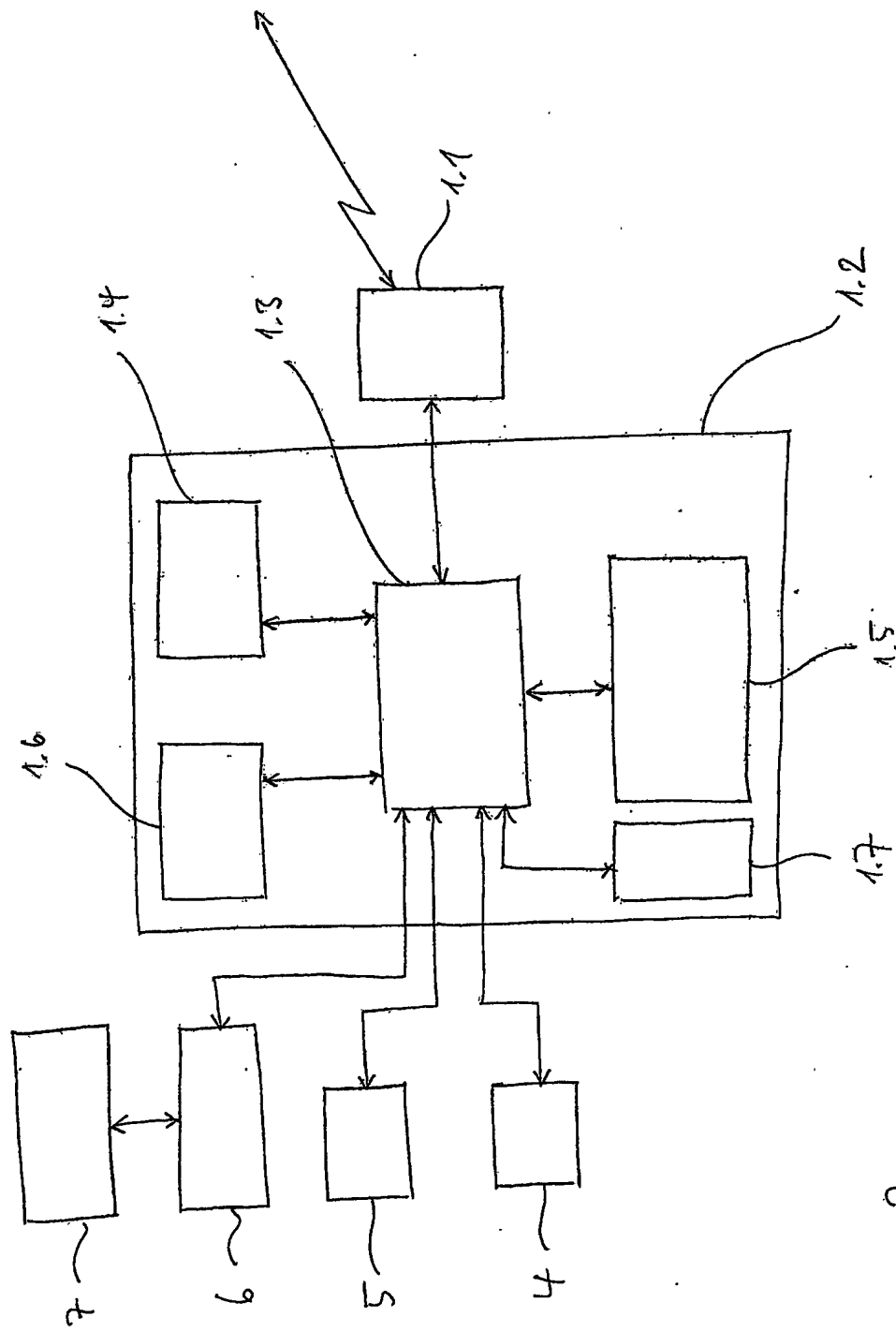


Fig. 2

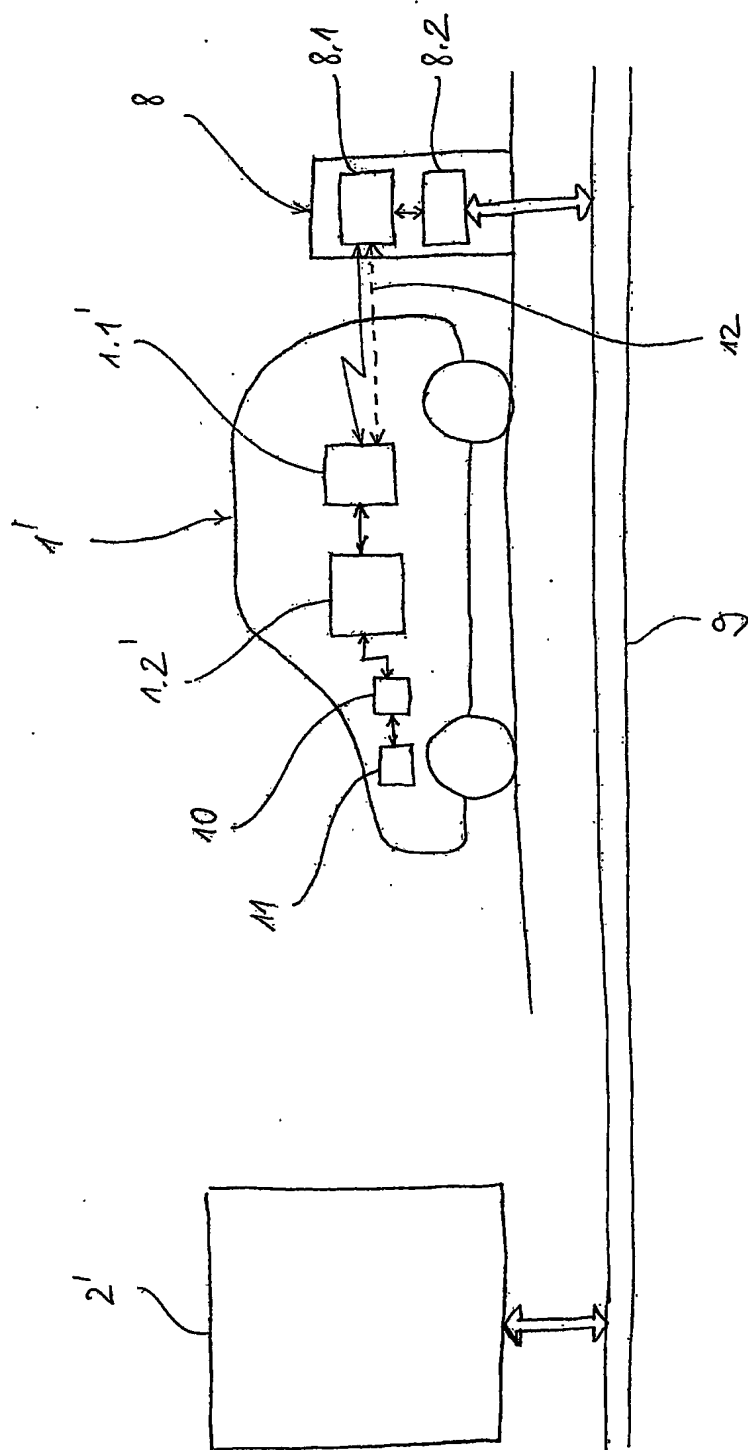


Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/EP2004/000505

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07B15/00 B60R16/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07B B60R H04L G06F G07F G08G B61L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/59711 A (RIEDER HELMUT ;EFKON AG (AT); PAMMER RAIMUND (AT)) 16 August 2001 (2001-08-16)	1-9, 11-23, 25,26, 28,35-37 10,24, 27,29-34
Y	abstract page 1, paragraph 1 page 3, last paragraph -page 4, paragraph 1 page 6, paragraph 3 -page 8, paragraph 1 figures 1,2 --- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the International filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

4 June 2004

Date of mailing of the international search report

17/06/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Kopp, K

INTERNATIONAL SEARCH REPORT

 International Application No
 PCT/04/000505

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/034301 A1 (ANDERSSON STEFAN) 21 March 2002 (2002-03-21) paragraph '0003! - paragraph '0004! paragraph '0006! - paragraph '0007! paragraph '0018! - paragraph '0022! paragraph '0029! - paragraph '0030! figure 3 claims 1,8 ---	1-4,6, 17-20,23
Y	EP 0 780 801 A (GZS GES FUER ZAHLUNGSSYSTEME M) 25 June 1997 (1997-06-25) page 12, line 46 - line 54 page 13, line 35 - line 38 page 15, line 26 -page 16, line 31 page 26, line 28 -page 27, line 53 page 35, line 21 -page 36, line 3 page 36, line 35 -page 37, line 13 page 38, line 8 - line 16 page 39, line 6 - line 13 ---	10,24, 27,29-34
A	WO 02/15149 A (NEW FLYER IND ;PACHET EUGENE (CA); HARVEY LEE (CA)) 21 February 2002 (2002-02-21) abstract page 1, line 9 - line 18 page 2, line 7 - line 8 page 2, line 16 -page 3, line 22 page 5, line 20 - line 25 page 7, line 22 -page 10, line 19 page 21, line 7 - line 11 figure 3A -----	1-37

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 4/000505

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0159711	A	16-08-2001	WO 0159711 A1	16-08-2001
			AT 1992000 A	15-01-2004
			AT 246384 T	15-08-2003
			AU 3347201 A	20-08-2001
			DE 50100441 D1	04-09-2003
			EP 1254434 A1	06-11-2002
			ES 2203590 T3	16-04-2004
			JP 2003526854 T	09-09-2003
			NO 20023718 A	06-08-2002
			PT 1254434 T	31-12-2003
			US 2003011494 A1	16-01-2003
			ZA 200205601 A	14-07-2003
US 2002034301	A1	21-03-2002	GB 2366139 A	27-02-2002
			AU 8394901 A	25-02-2002
			WO 0215626 A1	21-02-2002
			EP 1323323 A1	02-07-2003
EP 0780801	A	25-06-1997	AU 1432697 A	14-07-1997
			WO 9722953 A1	26-06-1997
			EP 0780801 A1	25-06-1997
WO 0215149	A	21-02-2002	AU 5808801 A	25-02-2002
			AU 6195001 A	25-02-2002
			AU 6195101 A	25-02-2002
			WO 0215149 A1	21-02-2002
			WO 0215150 A1	21-02-2002
			WO 0215151 A1	21-02-2002
			US 6556899 B1	29-04-2003
			US 6611739 B1	26-08-2003
			US 6681174 B1	20-01-2004

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 IPK 7 G07B15/00 B60R16/00 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 IPK 7 G07B B60R H04L G06F G07F G08G B61L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, COMPENDEX

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y	<p>WO 01/59711 A (RIEDER HELMUT ;EFKON AG (AT); PAMMER RAIMUND (AT)) 16. August 2001 (2001-08-16)</p> <p>Zusammenfassung Seite 1, Absatz 1 Seite 3, letzter Absatz -Seite 4, Absatz 1 Seite 6, Absatz 3 -Seite 8, Absatz 1 Abbildungen 1,2</p> <p style="text-align: center;">--- -/-</p>	<p>1-9, 11-23, 25, 26, 28, 35-37 10, 24, 27, 29-34</p>

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

G Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

4. Juni 2004

Absendedatum des internationalen Recherchenberichts

17/06/2004

Name und Postanschrift der internationalen Recherchenbehörde
 Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Kopp, K

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2002/034301 A1 (ANDERSSON STEFAN) 21. März 2002 (2002-03-21) Absatz '0003! - Absatz '0004! Absatz '0006! - Absatz '0007! Absatz '0018! - Absatz '0022! Absatz '0029! - Absatz '0030! Abbildung 3 Ansprüche 1,8 ----	1-4, 6, 17-20, 23
Y	EP 0 780 801 A (GZS GES FUER ZAHLUNGSSYSTEME M) 25. Juni 1997 (1997-06-25) Seite 12, Zeile 46 - Zeile 54 Seite 13, Zeile 35 - Zeile 38 Seite 15, Zeile 26 -Seite 16, Zeile 31 Seite 26, Zeile 28 -Seite 27, Zeile 53 Seite 35, Zeile 21 -Seite 36, Zeile 3 Seite 36, Zeile 35 -Seite 37, Zeile 13 Seite 38, Zeile 8 - Zeile 16 Seite 39, Zeile 6 - Zeile 13 ----	10, 24, 27, 29-34
A	WO 02/15149 A (NEW FLYER IND ;PACHET EUGENE (CA); HARVEY LEE (CA)) 21. Februar 2002 (2002-02-21) Zusammenfassung Seite 1, Zeile 9 - Zeile 18 Seite 2, Zeile 7 - Zeile 8 Seite 2, Zeile 16 -Seite 3, Zeile 22 Seite 5, Zeile 20 - Zeile 25 Seite 7, Zeile 22 -Seite 10, Zeile 19 Seite 21, Zeile 7 - Zeile 11 Abbildung 3A -----	1-37

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die der selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/04/000505

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0159711 A	16-08-2001	WO 0159711 A1	16-08-2001
		AT 1992000 A	15-01-2004
		AT 246384 T	15-08-2003
		AU 3347201 A	20-08-2001
		DE 50100441 D1	04-09-2003
		EP 1254434 A1	06-11-2002
		ES 2203590 T3	16-04-2004
		JP 2003526854 T	09-09-2003
		NO 20023718 A	06-08-2002
		PT 1254434 T	31-12-2003
		US 2003011494 A1	16-01-2003
		ZA 200205601 A	14-07-2003
US 2002034301 A1	21-03-2002	GB 2366139 A	27-02-2002
		AU 8394901 A	25-02-2002
		WO 0215626 A1	21-02-2002
		EP 1323323 A1	02-07-2003
EP 0780801 A	25-06-1997	AU 1432697 A	14-07-1997
		WO 9722953 A1	26-06-1997
		EP 0780801 A1	25-06-1997
WO 0215149 A	21-02-2002	AU 5808801 A	25-02-2002
		AU 6195001 A	25-02-2002
		AU 6195101 A	25-02-2002
		WO 0215149 A1	21-02-2002
		WO 0215150 A1	21-02-2002
		WO 0215151 A1	21-02-2002
		US 6556899 B1	29-04-2003
		US 6611739 B1	26-08-2003
		US 6681174 B1	20-01-2004

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
5. August 2004 (05.08.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/066219 A1

(51) Internationale Patentklassifikation⁷: **G07B 15/00**,
B60R 16/00, H04L 29/06

B SYSTEMS AG [DE/DE]; Öhderstrasse 4-4a, 42289
Wuppertal (DE).

(21) Internationales Aktenzeichen: PCT/EP2004/000505

(72) Erfinder; und

(22) Internationales Anmeldedatum:

22. Januar 2004 (22.01.2004)

(75) Erfinder/Anmelder (*nur für US*): **KAMPERT, Werner**
[DE/DE]; Alter Teichweg 9h, 22081 Hamburg (DE).
KNEE-FORREST, Paul [CZ/CZ]; Petra obravce 2261,
44001 Louny (CZ). **BIEBER, Wolf-Rüdiger** [DE/DE];
Brambecke 81, 42399 Wuppertal (DE). **STAMM, Egbert**
[DE/DE]; Küllersberg, 42653 Solingen (DE).

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:

103 02 449.2 22. Januar 2003 (22.01.2003) DE

103 50 647.0 29. Oktober 2003 (29.10.2003) DE

(74) **Anwalt: KARLHUBER, Mathias**; Cohausz & Florack,
Bleichstrasse 14, 40211 Düsseldorf (DE).

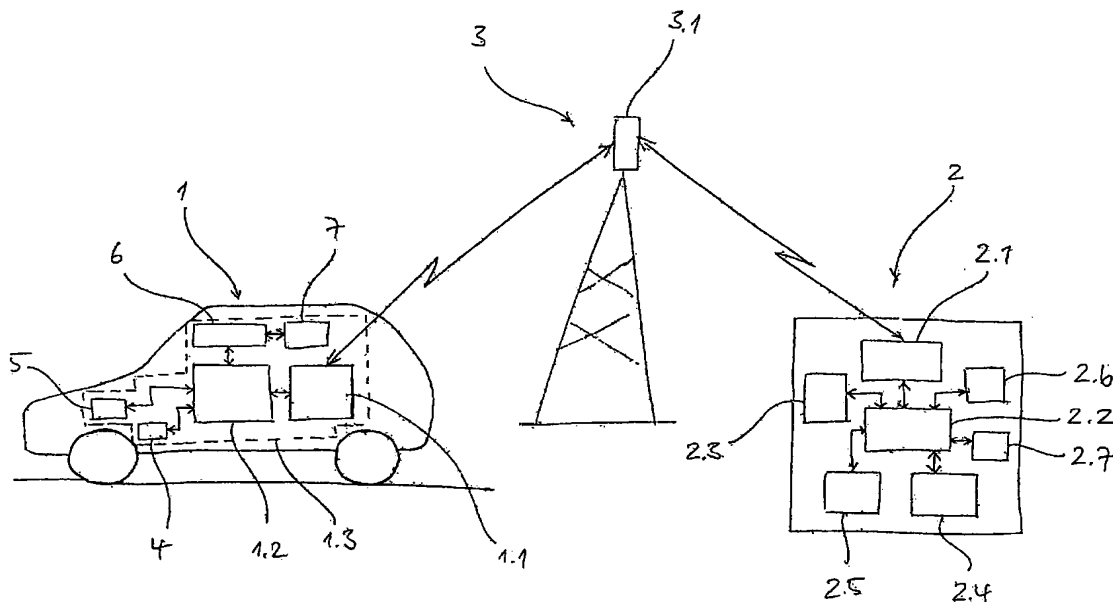
(71) **Anmelder (für alle Bestimmungsstaaten mit Ausnahme
von US): FRANCOTYP-POSTALIA AG & CO. KG**
[DE/DE]; Triftweg 21-26, 16547 Birkenwerder (DE).

(81) **Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart):** AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** MOBILE DATA TRANSMISSION METHOD AND SYSTEM

(54) **Bezeichnung:** VERFAHREN UND ANORDNUNG ZUR MOBILEN DATENÜBERTRAGUNG



(57) **Abstract:** The invention relates to a method for transmitting data between a mobile first device (1; 1'; 1"), particularly a vehicle, and a data center (2; 2') that is at least temporally remote from the first device (1; 1'; 1"). The transmission of the data ensues over at least one mobile first transmission device (1.1; 1.1'; 1.1"), and the transmitted data contain first data that are authenticated by cryptographic means.

(57) **Zusammenfassung:** Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1"), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1") zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1") erfolgt und die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.

WO 2004/066219 A1

From the International Bureau 21 JUL 2005

PCT

FIRST NOTICE INFORMING THE APPLICANT OF
THE COMMUNICATION OF THE INTERNATIONAL
APPLICATION (TO DESIGNATED OFFICES WHICH
DO NOT APPLY THE 30 MONTH TIME LIMIT
UNDER ARTICLE 22(1))

(PCT Rule 47.1(c))

To:

KARLHUBER, Mathias
Cohausz & Florack
Bleichstrasse 14
40211 Düsseldorf
ALLEMAGNE

Eingang:	06. SEP. 2004		
Frist bis:			
Bearbeiter	RA	Erreicht	Gesehen

Date of mailing (day/month/year)
26 August 2004 (26.08.2004)

Applicant's or agent's file reference
KAnw 030992WO

IMPORTANT NOTICE

International application No.
PCT/EP2004/000505

International filing date (day/month/year)
22 January 2004 (22.01.2004)

Priority date (day/month/year)
22 January 2003 (22.01.2003)

Applicant

FRANCOTYP-POSTALIA AG & CO. KG et al

- ATTENTION:** For any designated Office(s), for which the time limit under Article 22(1), as in force from 1 April 2002 (30 months from the priority date), **does apply**, please see Form PCT/IB/308(Second and Supplementary Notice) (to be issued promptly after the expiration of 28 months from the priority date).
- Notice is hereby given that the following designated Office(s), for which the time limit under Article 22(1), as in force from 1 April 2002, **does not apply**, has/have requested that the communication of the international application, as provided for in Article 20, be effected under Rule 93bis.1. The International Bureau has effected that communication on the date indicated below:
05 August 2004 (05.08.2004)

CH

In accordance with Rule 47.1(c-bis)(i), those Offices will accept the present notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

- The following designated Offices, for which the time limit under Article 22(1), as in force from 1 April 2002, **does not apply**, have not requested, as at the time of mailing of the present notice, that the communication of the international application be effected under Rule 93bis.1:

FI, LU, SE, TZ, UG, ZM

In accordance with Rule 47.1(c-bis)(ii), those Offices accept the present notice as conclusive evidence that the Contracting State for which that Office acts as a designated Office does not require the furnishing, under Article 22, by the applicant of a copy of the international application.

4. TIME LIMITS for entry into the national phase

For the designated Office(s) listed above, and unless a demand for international preliminary examination has been filed before the expiration of **19 months** from the priority date (see Article 39(1)), the applicable time limit for entering the national phase will, **subject to what is said in the following paragraph**, be **20 MONTHS** from the priority date.

In practice, **time limits other than the 20-month time limit** will continue to apply, for various periods of time, in respect of certain of the designated Offices listed above. For **regular updates on the applicable time limits** (20 or 21 months, or other time limit), Office by Office, refer to the *PCT Gazette*, the *PCT Newsletter* and the *PCT Applicant's Guide*, Volume II, National Chapters, all available from WIPO's Internet site, at <http://www.wipo.int/pct/en/index.html>.

It is the applicant's **sole responsibility** to monitor all these time limits.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Ellen Moyse

Facsimile No.+41 22 740 14 35

Facsimile No.+41 22 338 89 75

From the INTERNATIONAL BUREAU

PCT

SECOND AND SUPPLEMENTARY NOTICE
INFORMING THE APPLICANT OF THE
COMMUNICATION OF THE INTERNATIONAL
APPLICATION (TO DESIGNATED OFFICES
WHICH APPLY THE 30 MONTH TIME
LIMIT UNDER ARTICLE 22(1))

(PCT Rule 47.1(c))

To:

KARLHUBER, Mathias
Cohausz & Florack
Bleichstrasse 14
40211 Düsseldorf
ALLEMAGNE

Eingang:	01. JUNI 2005		
Für die:			
Bearbeitet:	KA	bn	Erledigt: Gesehen:

Date of mailing (day/month/year) 26 May 2005 (26.05.2005)		
Applicant's or agent's file reference KANw 030992WO		
IMPORTANT NOTICE		
International application No. PCT/EP2004/000505	International filing date (day/month/year) 22 January 2004 (22.01.2004)	Priority date (day/month/year) 22 January 2003 (22.01.2003)
Applicant FRANCOTYP-POSTALIA AG & CO. KG et al		

- ATTENTION:** For any designated Office(s), for which the time limit under Article 22(1), as in force from 1 April 2002 (30 months from the priority date), **does not apply**, please see Form PCT/IB/308(First Notice) issued previously.
- Notice is hereby given that the following designated Office(s), for which the time limit under Article 22(1), as in force from 1 April 2002, **does apply**, has/have requested that the communication of the international application, as provided for in Article 20, be effected under Rule 93bis.1. The International Bureau has effected that communication on the date indicated below:
05 August 2004 (05.08.2004)

AU, AZ, BY, CN, CO, DZ, EP, HU, KG, KP, KR, MD, MK, MZ, NA, RU, SY, TM, US

In accordance with Rule 47.1(c-bis)(i), those Offices will accept the present notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

- The following designated Offices, for which the time limit under Article 22(1), as in force from 1 April 2002, **does apply**, have not requested, as at the time of mailing of the present notice, that the communication of the international application be effected under Rule 93bis.1:

AE, AG, AL, AM, AP, AT, BA, BB, BG, BR, BW, BZ, CA, CR, CU, CZ, DK, DM, EA, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, ID, IL, IN, IS, JP, KE, KZ, LC, LK, LR, LS, LT, LV, MA, MG, MN, MW, MX, NI, NO, NZ, OA, OM, PG, PH, PL, PT, RO, SC, SD, SG, SK, SL, TJ, TN, TR, TT, UA, UZ, VC, VN, YU, ZA, ZW

In accordance with Rule 47.1(c-bis)(ii), those Offices accept the present notice as conclusive evidence that the Contracting State for which that Office acts as a designated Office does not require the furnishing, under Article 22, by the applicant of a copy of the international application.

4. TIME LIMITS for entry into the national phase

For the designated or elected Office(s) listed above, the applicable time limit for entering the national phase will, **subject to what is said in the following paragraph**, be **30 MONTHS** from the priority date.

In practice, **time limits other than the 30-month time limit** will continue to apply, for various periods of time, in respect of certain of the designated or elected Office(s) listed above. For **regular updates on the applicable time limits** (30 or 31 months, or other time limit), Office by Office, refer to the *PCT Gazette*, the *PCT Newsletter* and the *PCT Applicant's Guide*, Volume II, National Chapters, all available from WIPO's Internet site, at <http://www.wipo.int/pct/en/index.html>.

It is the applicant's **sole responsibility** to monitor all these time limits.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Ellen Moyse
Facsimile No.+41 22 740 14 35	Facsimile No.+41 22 338 89 75

Rec'd PCT/PTO 21 JUL 2003

PCT

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

Internationales Aktenzeichen

Internationales Anmeldedatum

Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts (falls gewünscht)
(max. 12 Zeichen) KA/nw 030992WO

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren und Anordnung zur mobilen Datenübertragung

Feld Nr. II ANMELDER

☐ Diese Person ist gleichzeitig Erfinder

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

Francotyp-Postalia AG & Co. KG
Triftweg 21-26
16547 Birkenwerder
DE

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit (Staat):

DE

Sitz oder Wohnsitz (Staat):

DE

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

B Systems AG
Öhderstr. 4 - 4a
42289 Wuppertal
DE

Diese Person ist:

☒ nur Anmelder

☐ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit (Staat):

DE

Sitz oder Wohnsitz (Staat):

DE

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

☒ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ODER ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als:

☒ Anwalt

☐ gemeinsamer Vertreter

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

KARLHUBER, Mathias
COHAUSZ & FLORACK
Bleichstr. 14
40211 Düsseldorf
DE

Telefonnr.:

+49 211 90 49 00

Telefaxnr.:

+ 49 111 90 49 049

Fernschreibnr.:

Registrierungsnr. des Anwalts beim Amt:

☐ Zustellanschrift: Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

Fortsetzung von Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER*Wird keines der folgenden Felder benutzt, so sollte dieses Blatt dem Antrag nicht beigelegt werden.*

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

KAMPERT, Werner
Alter Teichweg 9h
22081 Hamburg
DE

Diese Person ist:

☐ nur Anmelder☒ Anmelder und Erfinder☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit (Staat):

DE

Sitz oder Wohnsitz (Staat):

DE

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika☒ nur die Vereinigten Staaten von Amerika☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

KNEE-FORREST, Paul
Petra obrovce 2261
44001 Louny
CZ

Diese Person ist:

☐ nur Anmelder☒ Anmelder und Erfinder☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit (Staat):

CZ

Sitz oder Wohnsitz (Staat):

CZ

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika☒ nur die Vereinigten Staaten von Amerika☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

BIEBER, Wolf-Rüdiger
Brambecke 81
42399 Wuppertal
DE

Diese Person ist:

☐ nur Anmelder☒ Anmelder und Erfinder☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit (Staat):

DE

Sitz oder Wohnsitz (Staat):

DE

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika☒ nur die Vereinigten Staaten von Amerika☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

STAMM, Egbert
Küllersberg 6
42653 Solingen

Diese Person ist:

☐ nur Anmelder☒ Anmelder und Erfinder☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit (Staat):

DE

Sitz oder Wohnsitz (Staat):

DE

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika☒ nur die Vereinigten Staaten von Amerika☐ die im Zusatzfeld angegebenen Staaten☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem zusätzlichen Fortsetzungsblatt angegeben.

Feld Nr. V BESTIMMUNGEN

Die Einreichung dieses Antrags umfaßt gemäß Regel 4.9 Absatz a die Bestimmung aller Vertragsstaaten, für die der PCT am internationalen Anmeldedatum verbindlich ist, und insoweit verfügbar, für jede Art von Schutzrecht und sowohl für ein regionales als auch für ein nationales Patent.

Dennoch wird

- ☒ DE Deutschland nicht für ein nationales Schutzrecht bestimmt
☐ KR Republik Korea nicht für ein nationales Schutzrecht bestimmt
☐ RU Russische Föderation nicht für ein nationales Schutzrecht bestimmt

(Obenstehende Kästchen können angekreuzt werden, um die betreffenden Bestimmungen (unwiderruflich) auszuschließen, um zu vermeiden daß eine frühere nationale Anmeldung, deren Priorität beansprucht wird, nach nationalem Recht ihre Wirkung verliert. Siehe die Anmerkungen zu Feld Nr. V für die Folgen solcher nationalen Rechtsvorschriften in diesen und bestimmten anderen Staaten).

Feld Nr. VI PRIORITÄTSANSPRUCH

Die Priorität der folgenden früheren Anmeldung(en) wird hiermit in Anspruch genommen:

Anmeldedatum der früheren Anmeldung (Tag/Monat/Jahr)	Aktenzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine:		
		ationale Anmeldung: Staat oder Mitglied der WTO	regionale Anmeldung:* regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1) 22.01.03	103 02 449.2	DE		
Zeile (2) 29.10.03	103 50 647.0	DE		
Zeile (3)				

☐ Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.

Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln (nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist (sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist):

☐ sämtliche Zeilen ☐ Zeile (1) ☐ Zeile (2) ☐ Zeile (3) ☐ weitere, siehe Zusatzfeld

* Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, geben Sie mindestens einen Staat an, der Mitgliedstaat der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums oder Mitglied der Welthandelsorganisation ist und für den oder das die frühere Anmeldung eingereicht wurde:

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der internationalen Recherchenbehörde (ISA) (falls zwei oder mehr als zwei internationale Recherchenbehörden für die Ausführung der internationalen Recherche zuständig sind, geben Sie die von Ihnen gewählte Behörde an; der Zweibuchstaben-Code kann benutzt werden):

ISA / EP

Antrag auf Nutzung der Ergebnisse einer früheren Recherche; Bezugnahme auf diese frühere Recherche (falls eine frühere Recherche bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist):

Datum (Tag/Monat/Jahr)

Aktenzeichen

Staat (oder regionales Amt)

Feld Nr. VIII ERKLÄRUNGEN

Die Felder Nr. VIII (i) bis (v) enthalten die folgenden Erklärungen (Kreuzen Sie unten die entsprechenden Kästchen an und geben Sie in der rechten Spalte für jede Erklärung deren Anzahl an):

Anzahl der
Erklärungen

- ☐ Feld Nr. VIII (i) Erklärung hinsichtlich der Identität des Erfinders :
- ☐ Feld Nr. VIII (ii) Erklärung hinsichtlich der Berechtigung des Anmelders, zum Zeitpunkt des internationalen Anmeldedatums, ein Patent zu beantragen und zu erhalten :
- ☐ Feld Nr. VIII (iii) Erklärung hinsichtlich der Berechtigung des Anmelders, zum Zeitpunkt des internationalen Anmeldedatums, die Priorität einer früheren Anmeldung zu beanspruchen :
- ☐ Feld Nr. VIII (iv) Erfindererklärung (nur im Hinblick auf die Bestimmung der Vereinigten Staaten von Amerika) :
- ☐ Feld Nr. VIII (v) Erklärung hinsichtlich unschädlicher Offenbarungen oder Ausnahmen von der Neuheitsschädlichkeit :

Feld Nr. IX KONTROLLISTE; EINREICHUNGSSPRACHE

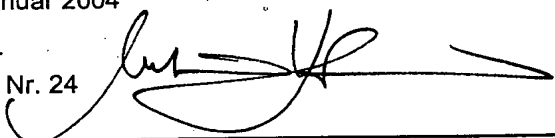
Diese internationale Anmeldung enthält:	Dieser internationalen Anmeldung liegen die folgenden Unterlagen bei (kreuzen Sie die entsprechenden Kästchen an und geben Sie in der rechten Spalte jeweils die Anzahl der beiliegenden Exemplare an)	Anzahl
(a) auf Papier, die folgende Anzahl Blätter:		
Antrag (inklusive Erklärungsblätter) :	1. <input checked="" type="checkbox"/> Blatt für die Gebührenberechnung :	
Beschreibung (ohne Sequenzprotokoll und/oder diesbezügliche Tabellen) :	2. <input type="checkbox"/> Original einer gesonderten Vollmacht :	
Ansprüche :	3. <input type="checkbox"/> Original einer allgemeinen Vollmacht :	
Zusammenfassung :	4. <input type="checkbox"/> Kopie der allgemeinen Vollmacht; Aktenzeichen (falls vorhanden) :	
Zeichnungen :	5. <input type="checkbox"/> Begründung für das Fehlen einer Unterschrift :	
Teilanzahl :	6. <input type="checkbox"/> Prioritätsbeleg(e), in Feld Nr. VI durch folgende Zeilennummer(n) gekennzeichnet :	
Sequenzprotokoll :	7. <input type="checkbox"/> Übersetzung der internationalen Anmeldung in die folgende Sprache :	
diesbezügliche Tabellen :	8. <input type="checkbox"/> Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material :	
(für beide, Anzahl der Blätter, soweit auf Papier eingereicht wird, unabhängig davon, ob zusätzlich auch in computerlesbarer Form eingereicht wird; siehe unter (c))	9. <input type="checkbox"/> Sequenzprotokoll in computerlesbarer Form (Art und Anzahl der Datenträger)	
Gesamtanzahl :	(i) <input type="checkbox"/> Kopie ausschließlich für die Zwecke der internationalen Recherche nach Regel 13ter (und nicht als Teil der internationalen Anmeldung) :	
	(ii) <input type="checkbox"/> (nur falls Felder (b)(i) oder (c)(i) in der linken Spalte angekreuzt wurden) zusätzliche Kopien einschließlich, soweit zutreffend, einer Kopie für die Zwecke der internationalen Recherche nach Regel 13ter :	
	(iii) <input type="checkbox"/> zusammen mit entsprechender Erklärung, daß die Kopie(n) mit dem in der linken Spalte aufgeführten Sequenzprotokoll identisch ist :	
	10. <input type="checkbox"/> Tabellen in computerlesbarer Form im Zusammenhang mit Sequenzprotokoll (Art und Anzahl der Datenträger)	
	(i) <input type="checkbox"/> Kopie ausschließlich für die Zwecke der internationalen Recherche nach Abschnitt 802(b-quater) (und nicht als Teil der internationalen Anmeldung) :	
	(ii) <input type="checkbox"/> (nur falls Felder (b)(ii) oder (c)(ii) in der linken Spalte angekreuzt wurden) zusätzliche Kopien einschließlich, soweit zutreffend, einer Kopie für die Zwecke der internationalen Recherche nach Abschnitt 802(b-quater) :	
	(iii) <input type="checkbox"/> zusammen mit entsprechender Erklärung, daß die Kopie(n) mit dem in der linken Spalte aufgeführten Tabellen identisch ist (sind) :	
	11. <input type="checkbox"/> Sonstige (einzeln auflisten) :	
Abbildung der Zeichnungen, die mit der Zusammenfassung veröffentlicht werden soll (Nr.): 1	Sprache, in der die internationale Anmeldung eingereicht wird: Deutsch	

Feld Nr. X UNTERSCHRIFT DES ANMELDERS, DES ANWALTS ODER DES GEMEINSAMEN VERTRETERS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Düsseldorf, 22. Januar 2004

 Mathias Karlhuber
 Zusammenschluß Nr. 24



Vom Anmeldeamt auszufüllen		2. Zeichnungen:
1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung:		
3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:		<input type="checkbox"/> nicht eingegangen:
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:		
5. Internationale Recherchenbehörde (falls zwei oder mehr zuständig sind): ISA /	6. <input type="checkbox"/> Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben	

Vom Internationalen Büro auszufüllen
Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
5. August 2004 (05.08.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/066219 A1

(51) Internationale Patentklassifikation⁷: G07B 15/00,
B60R 16/00, H04L 29/06

B SYSTEMS AG [DE/DE]; Öhderstrasse 4-4a, 42289
Wuppertal (DE).

(21) Internationales Aktenzeichen: PCT/EP2004/000505

(72) Erfinder; und

(22) Internationales Anmeldedatum:
22. Januar 2004 (22.01.2004)

(75) Erfinder/Anmelder (nur für US): KAMPERT, Werner
[DE/DE]; Alter Teichweg 9h, 22081 Hamburg (DE).
KNEE-FORREST, Paul [CZ/CZ]; Petra obravce 2261,
44001 Louny (CZ). BIEBER, Wolf-Rüdiger [DE/DE];
Brambecke 81, 42399 Wuppertal (DE). STAMM, Egbert
[DE/DE]; Küllersberg, 42653 Solingen (DE).

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 02 449.2 22. Januar 2003 (22.01.2003) DE
103 50 647.0 29. Oktober 2003 (29.10.2003) DE

(74) Anwalt: KARLHUBER, Mathias; Cohausz & Florack,
Bleichstrasse 14, 40211 Düsseldorf (DE).

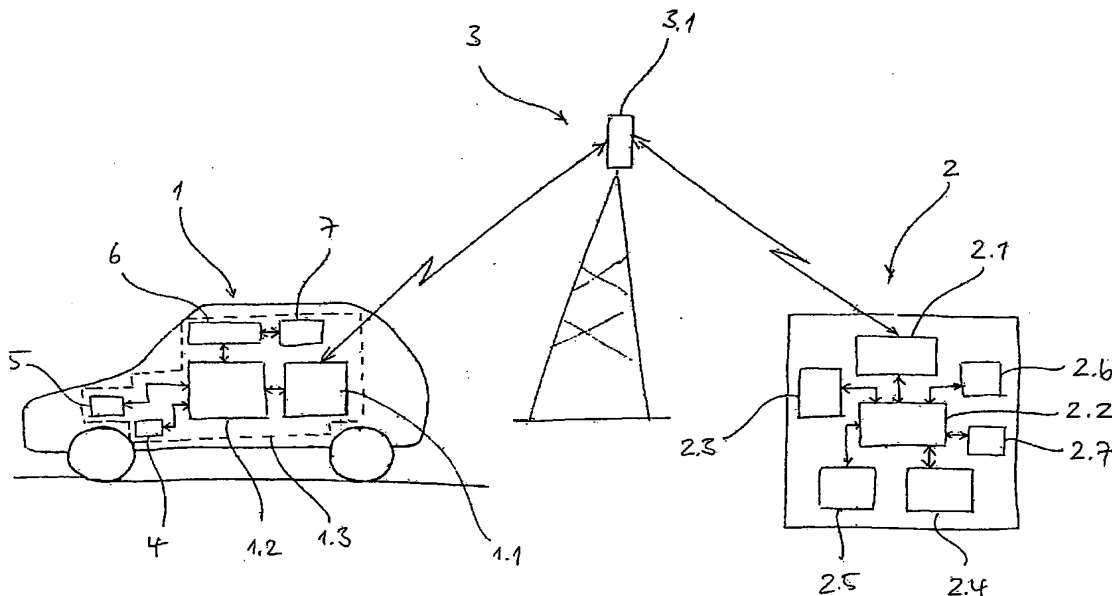
(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme
von US): FRANCOTYP-POSTALIA AG & CO. KG
[DE/DE]; Triftweg 21-26, 16547 Birkenwerder (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI,

[Fortsetzung auf der nächsten Seite]

(54) Title: MOBILE DATA TRANSMISSION METHOD AND SYSTEM

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR MOBILEN DATENÜBERTRAGUNG



(57) Abstract: The invention relates to a method for transmitting data between a mobile first device (1; 1'; 1''), particularly a vehicle, and a data center (2; 2') that is at least temporally remote from the first device (1; 1'; 1''). The transmission of the data ensues over at least one mobile first transmission device (1.1; 1.1'; 1.1''), and the transmitted data contain first data that are authenticated by cryptographic means.

(57) Zusammenfassung: Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1''), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') erfolgt und die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.

WO 2004/066219 A1

Verfahren und Anordnung zur mobilen Datenübertragung

Die vorliegende Erfindung betrifft ein Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale, wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung erfolgt. Sie betrifft weiterhin eine entsprechende Anordnung zum Übertragen von Daten.

Ein solches gattungsgemäßes Verfahren ist beispielsweise aus dem Bereich der Schienenverkehrstechnik bekannt. Dort werden zwischen dem Steuerrechner des Zuges über eine damit verbundene entsprechende Sender/Empfängereinheit des Zuges Daten mit einer externen Zugleitstelle ausgetauscht. Sofern es sich bei den ausgetauschten Daten um sicherheitsrelevante Daten handelt, wird durch entsprechend redundante Übertragungsprotokolle eine fehlerfreie Übertragung der die Daten repräsentierenden Signale sichergestellt bzw. werden nur solche Signale akzeptiert, deren Fehlerwahrscheinlichkeit innerhalb bestimmter Toleranzgrenzen liegt.

Ein Nachteil dieser bekannten Verfahren liegt darin, dass eine Absicherung der durch die Signale repräsentierten Daten gegen Manipulationen in der Regel nicht stattfindet. Bei der Übertragung der Daten zwischen dem Fahrzeug und der Datenzentrale könnte es somit problemlos zu wissentlichen und willentlichen Manipulationen kommen. Dies ist insbesondere dann von Nachteil, wenn diese Daten sicherheitsrelevante erste Daten umfassen. Um hier Manipulationen vorzubeugen, wäre es wünschenswert, eine entsprechende Absicherung solcher sicherheitsrelevanter erster Daten und damit einen Manipulationsschutz zu erzielen.

Weiterhin wäre es wünschenswert, das bekannte Verfahren auch in anderen Bereichen einsetzen zu können. Insbesondere wäre es wünschenswert, ein solches Verfahren bei der Überwachung anderer mobiler Einrichtungen einzusetzen. Hierzu zählt insbesondere die Überwachung von gemieteten oder geleasteten Fahrzeugen. Gerade hier stellt sich aber wieder das Problem, dass die übertragenen Daten, gerade wenn sie beispielsweise abrechnungsrelevante und damit sicherheitsrelevante erste Daten umfassen, mit dem bekannten Datenübertragungsverfahren vergleichsweise anfällig für Manipulationen sind.

Der vorliegenden Erfindung liegt daher die Aufgabe zu Grunde, ein Verfahren bzw. eine Anordnung der eingangs genannten Art zur Verfügung zu stellen, welches bzw. welche die oben genannten Nachteile nicht oder zumindest in geringerem Maß aufweist und, insbesondere bei der Übertragung, einen erhöhten Manipulationsschutz sicherheitsrelevanter Daten gewährleistet.

Die vorliegende Erfindung löst diese Aufgabe ausgehend von einem Verfahren gemäß dem Oberbegriff des Anspruchs 1 durch die im kennzeichnenden Teil des Anspruchs 1 angegebenen Merkmale. Sie löst diese Aufgabe weiterhin ausgehend von einer Anordnung gemäß dem Oberbegriff des Anspruchs 17 durch die im kennzeichnenden Teil des Anspruchs 17 angegebenen Merkmale.

Der vorliegenden Erfindung liegt die technische Lehre zu Grunde, dass man einen erhöhten Manipulationsschutz sicherheitsrelevanter erster Daten erzielt, wenn die übertragenen ersten Daten durch kryptographische Mittel authentifiziert werden. Die Authentifizierung bringt den Vorteil mit sich, dass auch zu einem späteren Zeitpunkt durch ein entsprechendes Verifizierungsverfahren zweifelsfrei nachgewiesen werden kann, dass die Daten während der Übertragung oder gegebenenfalls auch später nicht manipuliert wurden.

Die Authentifizierung durch kryptographische Mittel kann in beliebiger bekannter Weise erfolgen. So kann beispielsweise ein so genannter Message Authentication Code (MAC) verwendet werden. Ein solcher MAC wird in der Regel unter Verwendung eines so genannten geteilten Geheimnisses, in der Regel eines geheimen Schlüssels generiert, der sowohl der den MAC erzeugenden Einheit als auch der den MAC verifizierenden Einheit bekannt ist, ansonsten aber geheim gehalten wird. Die zu authentifizierenden Daten werden zusammen mit dem geheimen Schlüssel einem Berechnungsalgorithmus zugeführt, der hieraus den MAC generiert. Der Berechnungsalgorithmus ist so ausgebildet, dass der MAC ohne Kenntnis des geheimen Schlüssels ohne übermäßig hohen Berechnungsaufwand nicht aus den zu authentifizierenden Daten rekonstruiert werden kann. Üblicherweise schließt der Berechnungsalgorithmus einen so genannten Hash-Algorithmus (z. B. SHA-1, SHA-2, MD5 etc.) ein. Zur Verifizierung des MAC wird seitens der verifizierenden Einheit aus den zu authentifizierenden Daten zusammen mit dem geheimen Schlüssel unter Verwendung des selben Berechnungsalgorithmus ein zweiter MAC gebildet, der dann mit dem MAC verglichen wird, der den zu authentifizierenden Daten zugeordnet ist. Stimmen diese überein, sind die Daten authentisch.

Wegen der einfacheren Verwaltung der verwendeten kryptographischen Schlüssel, insbesondere der einfacheren Verteilung der öffentlichen Schlüssel, beispielsweise im Rahmen einer so genannten Public Key Infrastruktur (PKI), werden zur Authentifizierung der Daten vorzugsweise digitale Signaturen verwendet. Hierbei verschlüsselt die Einheit, welche die digitale Signatur erzeugt, die zu authentifizierenden Daten oder einen daraus generierten Wert mit einem privaten Schlüssel, der in der Regel nur ihr bekannt ist. Um die den zu authentifizierenden Daten zugeordnete Signatur zu verifizieren und damit die Authentizität der Daten zu überprüfen, entschlüsselt die verifizierende Einheit die Signatur mit einem ihr bekannten öffentlichen Schlüssel, der dem privaten Schlüssel zugeordnet ist. Das Ergebnis der Entschlüsselung wird dann mit den zu authentifizierenden Daten oder einem Wert, der daraus nach dem bei der Verschlüsselung verwendeten Algorithmus generiert wurde. Stimmen diese überein, sind die Daten authentisch.

Bei den zu authentifizierenden ersten Daten kann es sich grundsätzlich um beliebige Daten handeln. So kann es sich um beliebige Daten handeln, die von entsprechenden Einrichtungen der ersten Einrichtung bzw. der Datenzentrale erfasst oder generiert wurden. Insbesondere kann es sich um beliebige Daten handeln, die von entsprechenden Erfassungseinrichtungen der mobilen ersten Einrichtung erfasst wurden. Hierzu zählen unter anderem beliebige Messdaten, die über beliebige Messeinrichtungen gemessen wurden.

Vorzugsweise wird zusammen mit diesen Daten auch ihre jeweilige Quelle authentifiziert. Hierzu ist bevorzugt vorgesehen, dass die ersten Daten zur Authentifizierung einer ersten Quelle der ersten Daten wenigstens eine erste Quellenidentifikation umfassen. Diese erste Quellenidentifikation ist der ersten Quelle bevorzugt eindeutig zugeordnet. Es handelt sich vorzugsweise um eine einmalige und eindeutige Identifikation. Bei der ersten Quelle, die über die erste Quellenidentifikation identifiziert wird, kann es sich um die Einrichtung handeln, welche die ersten Daten erfasst bzw. generiert hat. So kann die erste Quelle beispielsweise ein Messaufnehmer oder Sensor sein, der die ersten Daten generiert. Ebenso kann es sich bei der ersten Quelle um eine Einrichtung handeln, über welche die ersten Daten im weiteren Verlauf geleitet werden. Dies ist insbesondere dann sinnvoll, wenn die ersten Daten durch diese Einrichtung eine Bearbeitung, eine Modifikation oder dergleichen erfahren. So kann die erste Quelle beispielsweise die Einrichtung sein, in der die ersten Daten authentifiziert werden. Ebenso kann es sich bei der ersten Quelle um eine Einrichtung handeln, über welche die ersten Daten übertragen werden.

Ein weiterer Vorteil dieser Variante liegt darin, dass durch die eindeutige Zuordnung der Daten zu der jeweiligen ersten Quelle anhand der authentifizierten Daten zu einem späteren

Zeitpunkt eine Aussage über die Qualität und die Leistungsfähigkeit der ersten Quelle getroffen werden kann. Dies gilt insbesondere dann, wenn eine längere Reihe von entsprechenden authentifizierten Daten zur Verfügung steht, sodass eine entsprechende Historie über die Leistung der ersten Quelle erstellt werden kann, aus der entsprechende Rückschlüsse gezogen werden können.

Die erste Quelle kann Bestandteil der ersten Einrichtung, der ersten Übertragungseinrichtung, der Datenzentrale oder jeder weiteren Einrichtung sein, über welche die Datenübertragung erfolgt. Vorzugsweise umfassen die ersten Daten jeweils eine Quellenidentifikation für sämtliche Stationen, welche die ersten Daten bei der Übertragung durchlaufen, um ihren Übertragungsweg zu einem späteren Zeitpunkt lückenlos nachvollziehen zu können.

Bei besonders vorteilhaften Ausgestaltungen des erfindungsgemäßen Verfahrens wird zudem auch der Empfänger der ersten Daten authentifiziert. Hierdurch ist es möglich, zu einem späteren Zeitpunkt den Nachweis zu führen, welche Daten an einen bestimmten Empfänger übergeben wurden. Dies ist insbesondere dann von Bedeutung, wenn der Empfang der ersten Daten die Erfüllung einer bestimmten entgeltspflichtigen Leistung darstellt. Durch die erfindungsgemäße Authentifizierung des Empfängers kann dann in vorteilhafter Weise zu einem späteren Zeitpunkt der Empfänger der ersten Daten und damit der Leistung nachgewiesen werden. Erfindungsgemäß ist hierzu bevorzugt vorgesehen, dass die ersten Daten zur Authentifizierung eines ersten Empfängers der ersten Daten eine erste Empfängeridentifikation umfassen.

Je nach Übertragungsrichtung kann der Empfänger Bestandteil der ersten Einrichtung, der ersten Übertragungseinrichtung, der Datenzentrale oder jeder weiteren Einrichtung sein, über welche die Datenübertragung erfolgt. Analog zu der oben geschilderten Quellenidentifikation ist vorzugsweise vorgesehen, dass die ersten Daten eine Empfängeridentifikation für jeden Empfänger aufweist, über den die Übertragung erfolgt. Bei Zwischenstationen in der Übertragung entspricht die Empfängeridentifikation dann in der Regel der Quellenidentifikation, sodass für solche Zwischenstationen lediglich eine einzige Identifikation in die ersten Daten aufgenommen werden muss.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahrens wird zusätzlich die Übertragung selbst bzw. ein Merkmal dieser Übertragung authentifiziert. Hierdurch ist es zu einem späteren Zeitpunkt möglich, gegebenenfalls nicht nur die Daten und die beteiligten Kommunikationspartner zweifelsfrei zu identifizieren. Es ist hiermit auch möglich, den Vorgang der Übertragung selbst zu identifizieren und/oder seine Qualität zu bewerten. So kann

die Übertragung beispielsweise durch ein entsprechendes zeitliches Merkmal in eine Reihenfolge von Übertragungen eingeordnet werden, um eine Historie der Übertragungen bzw. der übertragenen Daten zu erstellen. Ebenso kann die Übertragung durch ein entsprechendes Qualitätsmerkmal, beispielsweise das Signal-Rausch-Verhältnis, die Anzahl der Verbindungsversuche, Art und/oder Anzahl von aufgetretenen Fehlern etc., später hinsichtlich ihrer Qualität beurteilt werden. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten zur Authentifizierung der Übertragung der ersten Daten eine Übertragungsidentifikation umfassen. Diese Übertragungsidentifikation kann beispielsweise eine fortlaufende Übertragungsnummer umfassen, welche die Übertragung beispielsweise zusammen mit den Identifikationen der Kommunikationspartner eindeutig identifiziert. Eine exakte zeitliche Einordnung der Übertragung ist möglich, wenn die Übertragungsidentifikation eine absolute Zeitinformation hinsichtlich Beginn und/oder Ende der Übertragung umfasst.

Bei weiteren bevorzugten Varianten des erfindungsgemäßen Verfahrens werden zeitliche Ereignisse authentifiziert. Erfindungsgemäß umfassen die ersten Daten hierzu wenigstens eine für ein vorgebbares Ereignis charakteristische Zeitkennung. Bei den vorgebbaren Ereignis kann es sich beispielsweise um die Generierung bzw. Erfassung der zu übertragenen Daten handeln, ebenso kann es sich um das Senden bzw. Empfangen der ersten Daten handeln. Vorzugsweise ist jeweils eine Zeitkennung für einen dieser Vorgänge vorgesehen. Mit anderen Worten umfassen die ersten Daten beispielsweise eine erste Zeitkennung, die für den Zeitpunkt der Generierung bzw. Erfassung der zu übersenden Daten repräsentativ ist, eine zweite Zeitkennung, die für das Senden dieser Daten repräsentativ ist, und eine dritte Zeitkennung, die für das Empfangen dieser Daten repräsentativ ist.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass die authentifizierten ersten Daten in einen Protokolldatensatz eingefügt werden, der in der ersten Einrichtung und zusätzlich oder alternativ in der Datenzentrale gespeichert wird. Dieser Protokolldatensatz ermöglicht es gegebenenfalls beiden Kommunikationspartnern ohne weiteres zu einem beliebigen späteren Zeitpunkt die entsprechend authentifizierten Daten zu verifizieren.

Besonders günstige Varianten des erfindungsgemäßen Verfahrens zeichnen sich dadurch aus, dass mit ihnen eine zuverlässige Überwachung bestimmter Zustände, insbesondere bestimmter Zustände der mobilen ersten Einrichtung möglich ist. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer

ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung der ersten Einrichtung erfasst wurde.

Bei der Erfassungsgröße kann es sich grundsätzlich um eine beliebige durch entsprechende Erfassungseinrichtungen erfassende Größe handeln. So kann es sich beispielsweise um
5 eine Zustandsgröße der Umgebung der mobilen ersten Einrichtung handeln, welche durch entsprechende Sensoren oder dergleichen der mobilen ersten Einrichtung erfasst wird. Besonders vorteilhaft lässt sich das erfindungsgemäßen Verfahren jedoch zur Überwachung des Zustands der mobilen Einrichtung selbst einsetzen. Bevorzugt handelt es sich bei der ersten Erfassungsgröße daher um eine Zustandsgröße der ersten Einrichtung. Diese Zu-
10 standgröße kann beispielsweise ein Betriebsparameter der ersten Einrichtung sein. Hierzu zählen beispielsweise die Geschwindigkeit und die Beschleunigung der ersten Einrichtung, die nach Betrag und Richtung erfasst werden können. Ebenso kann natürlich auch die Position der ersten Einrichtung die erste Erfassungsgröße bilden. Ebenso kann es sich um eine Temperatur handeln, wie z. B. die Temperatur im Kühlwasser- oder Motorölkreislauf etc.
15 Schließlich kann es sich um einen Ölstand, den Reifendruck oder einen beliebigen anderen Zustandsparameter handeln. Es versteht sich im übrigen, dass beliebige Kombinationen solche Erfassungsgrößen über entsprechende Erfassungseinrichtungen erfasst und übermittelt werden können, um den Zustand der ersten Einrichtung zu charakterisieren.

Weitere vorteilhafte Varianten des erfindungsgemäßen Verfahrens ermöglichen eine Beeinflussung bestimmter Betriebsparameter und damit des Betriebs der mobilen ersten Einrichtung. Erfindungsgemäß ist hierzu vorgesehen, dass die ersten Daten wenigstens Betriebsbeeinflussungsdaten umfassen, die zur Beeinflussung des Betriebs der ersten Einrichtung an die erste Einrichtung übermittelt werden. So ist es beispielsweise möglich, durch die
20 Übertragung der ersten Daten zur ersten Einrichtung aktuelle Betriebsparameter zu verändern. Ebenso kann beispielsweise ein Austausch von Teilen der Betriebssoftware der ersten Einrichtung bis hin zum kompletten Austausch der Betriebssoftware vorgenommen werden. Mit der erfindungsgemäßen Authentifizierung der ersten Daten kann, gegebenenfalls zusammen mit anderen Sicherungsmechanismen, sichergestellt werden, dass nur authentische und autorisierte Daten berücksichtigt werden. Es kann damit also mit anderen Worten
30 nur zu einer autorisierten Beeinflussung des Betriebs der mobilen ersten Einrichtung erfolgen.

Bei weiteren vorteilhaften Varianten des erfindungsgemäßen Verfahrens werden die Daten über wenigstens eine zweite Datenübertragungseinrichtung übertragen. Diese zweite Datenübertragungseinrichtung kann sowohl ebenfalls mobil als auch stationär sein. Hierdurch

ist es möglich, ein kostengünstiges Übertragungssystem zu realisieren. So kann die zweite Datenübertragungseinrichtung entsprechend leistungsfähig ausgebildet sein, um die ersten Daten über eine weite Strecke zu und von der Datenzentrale zu übertragen. Die erste Datenübertragungseinrichtung kann dann einfacher und kostengünstiger gestaltet werden. Insbesondere kann sie für eine kürzere Übertragungsstrecke zur zweiten Datenübertragungseinrichtung ausgelegt werden. In einem solchen System kann beispielsweise ein ausreichend flächendeckendes Netz von zweiten Datenübertragungseinrichtungen realisiert werden, wobei sich eine erste Datenübertragungseinrichtung und eine zweite Datenübertragungseinrichtung dann lediglich ausreichend nahe kommen müssen, um die Übertragung zwischen der mobilen ersten Einrichtung der entfernten Datenzentrale sicherzustellen.

Die vorliegende Erfindung betrifft weiterhin ein Verfahren zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, bei dem zwischen der mobilen ersten Einrichtung und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale über wenigstens eine mobile erste Übertragungseinrichtung erste Daten mit dem oben beschriebenen erfindungsgemäßen Verfahren übertragen werden. Erfindungsgemäß umfassen die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten. Die ersten Überwachungsdaten umfassen wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße, der von einer ersten Erfassungseinrichtung der ersten Einrichtung erfasst wurde. Diese ersten Überwachungsdaten werden in der Datenzentrale verifiziert. Schließlich werden die ersten Überwachungsdaten bei erfolgreicher Verifikation in der Datenzentrale analysiert.

Vorzugsweise wird in der Datenzentrale in Abhängigkeit von der Analyse der ersten Überwachungsdaten eine erste Überwachungsreaktion ausgelöst. Bei der Überwachungsreaktion kann es sich grundsätzlich um eine beliebige Reaktion handeln.

Bei besonders vorteilhaften Varianten des erfindungsgemäßen Verfahren handelt es sich bei der Überwachungsreaktion um eine Abrechnung handeln. So kann beispielsweise bei der Überwachung der Nutzung von gemieteten oder geleasten mobilen Einheiten, beispielsweise Fahrzeugen, Baumaschinen etc., in Abhängigkeit von der über entsprechende Erfassungseinrichtungen erfassten, übermittelten und analysierten abrechnungsrelevanten Nutzung eine Abrechnung der Nutzung erfolgen. Durch die erfindungsgemäße Authentifizierung der übermittelten Daten ist dabei sichergestellt, dass diese während der Übertragung nicht manipuliert wurden. Erfindungsgemäß ist hierzu vorgesehen, dass die erste Überwachungsreaktion einen Abrechnungsvorgang umfasst.

Zusätzlich oder alternativ können auch beliebige andere Überwachungsreaktionen ausgelöst werden. So können beispielsweise im Rahmen der Überwachung des Betriebszustands von mobilen Einrichtungen so genannte Frühwarnsysteme realisiert werden. Werden beispielsweise über die ersten Daten Fehler oder kritische Zustände bestimmter Einheiten der ersten
5 Einrichtung erfasst oder ergibt sich aus der Analyse der ersten Daten, dass derartige Fehler oder kritische Zustände, gegebenenfalls mit einer bestimmten Wahrscheinlichkeit, innerhalb eines bestimmten Zeitraums eintreten, so kann als Überwachungsreaktion eine entsprechende Mitteilung an die erste Einrichtung übermittelt werden. Die erste Einrichtung kann diese Nachricht dann an den aktuellen Nutzer über eine entsprechend Schnittstelle, beispielsweise optisch und/oder akustisch ausgeben. Es versteht sich, dass diese Nachricht
10 dabei in der oben beschriebenen Weise entsprechend authentifiziert übermittelt werden kann, um Manipulationen auszuschließen. Zusätzlich oder alternativ kann eine solche Nachricht von der Datenzentrale auch automatisch, beispielsweise per Mobilfunk, an einen entsprechend registrierten Nutzer übermittelt werden.

15 Es versteht sich jedoch, dass nicht nur für die Funktion der mobilen Einheit unmittelbar relevante Erfassungsgrößen erfasst werden können. Mit anderen Worten können beispielsweise auch andere Erfassungsgrößen erfasst werden, welche keinen unmittelbaren Einfluss auf die Funktionsfähigkeit der mobilen Einheit haben.

So kann beispielsweise im Fall von gemieteten oder geleasten mobilen Einheiten die aktuelle Nutzung überwacht werden und als eine Überwachungsreaktion eine entsprechende
20 Nachricht generiert werden, sobald der Nutzer den vereinbarten Nutzungsrahmen überschreitet oder zu überschreiten droht. Ebenso kann bei Überschreiten des vereinbarten Nutzungsrahmens als Überwachungsreaktion auf einen anderen Abrechnungsmodus umgeschaltet werden. War beispielsweise bei einem gemieteten Fahrzeug eine bestimmte Kilometerleistung pauschal vergütet, kann bei Erfassung des Überschreitens dieser Kilometerleistung auf eine kilometerbezogene Abrechnung der Mehrkilometer umgeschaltet werden.
25

Ebenso kann beispielsweise gemieteten oder geleasten Fahrzeugen oder Maschinen die Position als erste Erfassungsgröße überwacht und analysiert werden. Verstößt der Nutzer gegen eine Vereinbarung, indem das Fahrzeug beispielsweise einen vereinbarten Einsatzbereich verlässt, oder droht ein solcher Verstoß, so kann ebenfalls eine entsprechende
30 Nachricht bzw. Warnung als Überwachungsreaktion übermittelt werden.

Weiterhin kann beispielsweise im Rahmen der Überwachung vorgeschriebener Ruhezeiten für Fahrzeugführer die Betriebsdauer anhand entsprechender Kriterien überwacht werden.

Ergibt sich anhand einer oder mehrerer Erfassungsgrößen, dass die vorgeschriebenen Ruhezeiten nicht eingehalten werden bzw. ein Verstoß hiergegen droht, so kann ebenfalls eine entsprechende Nachricht bzw. Warnung als Überwachungsreaktion übermittelt werden.

5 Der beiden vorgenannten Fällen können im Fall des Verstoßes unter bestimmten Voraussetzungen als weitere Überwachungsreaktion Gegenmaßnahmen eingeleitet werden. Im einfachsten Fall kann dies durch eine entsprechende Mitteilung an eine hoheitliche Einrichtung, wie beispielsweise die Polizei oder dergleichen, übermittelt werden, um den Verstoß abzustellen.

10 Ebenso kann aber unter Berücksichtigung entsprechender Sicherheitsvorschriften als Überwachungsreaktion eine direkte Beeinflussung der ersten Einrichtung erfolgen. Diese kann gegebenenfalls bis hin zur kontrollierten Abschaltung der ersten Einrichtung reichen.

Eine solche Beeinflussung kann natürlich auch im Fall der oben genannten Überwachungsfunktionsrelevanter Erfassungsgrößen erfolgen. Vorzugsweise ist daher vorgesehen, dass die erste Überwachungsreaktion die Generierung von Betriebsbeeinflussungsdaten umfasst, 15 die zur Beeinflussung des Betriebs der ersten Einrichtung an die erste Einrichtung übermittelt werden. Wird beispielsweise erfasst, dass für einen bestimmten Betriebsparameter ein kritischer Zustand droht oder vorliegt, können unter Berücksichtigung entsprechender Sicherheitsvorschriften entsprechende Gegenmaßnahmen eingeleitet werden, um diesen kritischen Zustand zu verhindern oder abzustellen. Hierbei ist es unter anderem auch möglich, 20 schadhafte Betriebssoftware oder Teile über eine solche Betriebsbeeinflussung zu warten oder gegebenenfalls sogar vollständig auszutauschen.

In allen vorgenannten Fällen mit entsprechenden Überwachungsreaktionen stellt die Authentifizierung der im Rahmen der Überwachungsreaktion an die mobile Einheit übermittelten ersten Daten sicher, dass es im Rahmen einer solchen Überwachungsreaktion zu kei- 25 nen nicht autorisierten Manipulationen kommen kann, sondern lediglich Prozesse ablaufen, die auf entsprechend autorisierten Daten basieren.

Bei weiteren bevorzugten Varianten des erfindungsgemäßen Verfahrens ist vorgesehen, dass bei der Analyse weitere, nicht von der ersten Einrichtung übermittelte Daten berücksichtigt werden. Hierbei kann es sich beispielsweise um statistische Daten handeln, welche 30 durch die Auswertung der Daten gewonnen wurden, die von baugleichen oder ähnlichen ersten Einrichtungen stammen. Ebenso kann es sich aber um, auf anderem Wege zu Datenzentrale gelangte Daten handeln. Insbesondere können bei der Auslösung einer Überwachungsreaktion auch externe Informationen hinsichtlich der ersten Einrichtung berücksichtigt

werden. So kann zum Beispiel eine der oben beschriebenen Überwachungsreaktionen ausgelöst werden, wenn in der Datenzentrale eine Information eingeht, dass die erste Einrichtung gestohlen wurde oder dergleichen.

5 Die vorliegende Erfindung betrifft weiterhin eine Anordnung zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung zumindest zeitweise entfernten Datenzentrale, wobei zur Übertragung der Daten wenigstens eine mobile erste Übertragungseinrichtung vorgesehen ist. Erfindungsgemäß umfassen die übertragenen Daten erste Daten und es ist wenigstens eine Sicherheitseinrichtung vorgesehen, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist. Die erfindungsgemäße Anordnung eignet sich zur Durchführung des erfindungsgemäßen Verfahrens. Mit ihr lassen sich die vorstehend beschriebenen Ausgestaltungen und Vorteile in derselben Weise realisieren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird.

15 Die Sicherheitseinrichtung umfasst dabei ein Kryptographiemodul, welches die oben beschriebenen kryptographischen Mittel zur Verfügung stellt. Die Sicherheitseinrichtung kann dabei insbesondere zur oben beschriebenen Generierung eines MAC ausgebildet sein. Vorzugsweise ist die Sicherheitseinrichtung zur Bildung einer ersten digitalen Signatur unter Verwendung der ersten Daten ausgebildet, um die ersten Daten zu authentifizieren.

20 Das Kryptographiemodul kann sowohl zur Verschlüsselung zu speichernder Daten verwendet werden als auch zur Verschlüsselung zu übertragender Daten. Es versteht sich, dass je nach Anwendung, also beispielsweise je nachdem, ob Daten versandt oder gespeichert werden sollen, auch unterschiedliche kryptographische Verfahren angewendet werden können.

25 Neben dem bzw. den kryptographischen Algorithmen und einem oder mehreren entsprechenden kryptographischen Schlüsseln umfassen die Kryptographiedaten das Kryptographiemoduls bevorzugt weitere Daten, wie beispielsweise ein oder mehrere kryptographische Zertifikate entsprechender Zertifizierungsinstanzen sowie gegebenenfalls ein oder mehrere eigene kryptographische Zertifikate der Sicherheitseinrichtung.

30 Vorzugsweise ist die Sicherheitseinrichtung zum Austausch wenigstens eines Teils der Kryptographiedaten ausgebildet, um in vorteilhafter Weise eine einfache und dauerhaft zuverlässige Sicherung der Daten zu gewährleisten. Hierbei kann insbesondere vorgesehen sein, dass neben den kryptographischen Schlüsseln und kryptographischen Zertifikaten

auch der jeweils verwendete kryptographische Algorithmus ausgetauscht werden kann, um das System in einfacher Weise an geänderte Sicherheitsanforderungen anpassen zu können. Die Implementierung und der Austausch der Kryptographiedaten erfolgt bevorzugt im Rahmen einer so genannten Public Key Infrastruktur (PKI), wie sie hinlänglich bekannt ist und daher an dieser Stelle nicht weiter beschrieben werden soll. Es versteht sich insbesondere, dass eine entsprechende Routine zur Überprüfung der Validität der verwendeten kryptographischen Zertifikate vorgesehen ist. Geeignete derartige Überprüfungsroutinen sind ebenfalls hinlänglich bekannt und sollen daher hier nicht näher beschrieben werden

Vorzugsweise ist die Sicherheitseinrichtung zur oben beschriebenen Authentifizierung einer ersten Quelle der ersten Daten ausgebildet. Hierzu ist die Sicherheitseinrichtung bevorzugt zum Einbringen einer ersten Quellenidentifikation in den ersten Datensatz ausgebildet. Weiter vorzugsweise ist die Sicherheitseinrichtung zur oben beschriebenen Authentifizierung eines ersten Empfängers der ersten Daten ausgebildet. Hierzu ist sie vorzugsweise zum Einbringen einer ersten Empfängeridentifikation in den ersten Datensatz ausgebildet.

Bei bevorzugten Varianten der erfindungsgemäßen Anordnung ist die Sicherheitseinrichtung zur Authentifizierung der Übertragung der ersten Daten ausgebildet. Hierzu ist sie bevorzugt zum Einbringen einer Übertragungsidentifikation in den ersten Datensatz ausgebildet. Weiterhin ist die Sicherheitseinrichtung vorzugsweise zum Einbringen wenigstens einer für ein vorgebbares Ereignis charakteristischen Zeitkennung in den ersten Datensatz ausgebildet.

Bei weiteren vorteilhaften Varianten der erfindungsgemäßen Anordnung ist vorgesehen, dass die Sicherheitseinrichtung zum Einbringen der authentifizierten ersten Daten in einen Protokolldatensatz ausgebildet ist. Die erste Einrichtung weist dann einen ersten Protokollspeicher zum Speichern des Protokolldatensatzes auf. Zusätzlich oder alternativ weist die Datenzentrale einen zweiten Protokollspeicher zum Speichern des Protokolldatensatzes auf.

Die Sicherheitseinrichtung kann grundsätzlich an beliebiger Stelle in der Übertragungsstrecke angeordnet sein. Bevorzugt umfasst die erste Einrichtung eine erste derartige Sicherheitseinrichtung. Zusätzlich oder alternativ umfasst die Datenzentrale eine zweite derartige Sicherheitseinrichtung.

Bei vorteilhaften Varianten der erfindungsgemäßen Anordnung umfassen die ersten Daten von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten. Diese Überwachungsdaten umfassen wiederum wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße. Die erste Einrichtung umfasst weiterhin eine erste Erfassungsein-

richtung zur Erfassung des ersten Erfassungswerts. Bei den Erfassungsgrößen kann es sich, wie oben erwähnt, um beliebige erfassbare Größen handeln. Bevorzugt ist die erste Erfassungseinrichtung zur Erfassung einer Zustandsgröße der ersten Einrichtung als erster Erfassungsgröße ausgebildet.

- 5 Bei weiteren bevorzugten Varianten der erfindungsgemäßen Anordnung ist vorgesehen, dass die ersten Daten von der Datenzentrale zur ersten Einrichtung übertragene Betriebsbeeinflussungsdaten umfassen. Die erste Einrichtung umfasst dann eine Betriebsbeeinflussungseinrichtung, um hierüber den Betrieb der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten zu beeinflussen, wie dies oben im Zusammenhang mit dem
- 10 erfindungsgemäßen Verfahren beschrieben wurde.

Die vorliegende Erfindung betrifft weiterhin eine Anordnung zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, mit einer erfindungsgemäßen Anordnung zur Übertragung von ersten Daten. Die ersten Daten umfassen dabei von der ersten Einrichtung zur Datenzentrale übertragene erste Überwachungsdaten, die wenigstens einen

15 ersten Erfassungswert einer ersten Erfassungsgröße umfassen. Die erste Einrichtung umfasst weiterhin eine erste Erfassungseinrichtung zur Erfassung des ersten Erfassungswerts. Die Datenzentrale weist eine zweite Sicherheitseinrichtung zum Verifizieren der ersten Überwachungsdaten auf. Weiterhin weist die Datenzentrale eine mit der zweiten Sicherheitseinrichtung verbundene Analyseeinrichtung zum Analysieren der ersten Überwachungsda-

20 ten in Abhängigkeit vom Ergebnis der Verifikation auf. Diese erfindungsgemäße Anordnung eignet sich zur Durchführung des erfindungsgemäßen Verfahrens zur Überwachung einer mobilen ersten Einrichtung. Mit ihr lassen sich die vorstehend beschriebenen Ausgestaltungen und Vorteile in derselben Weise realisieren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird.

- 25 Bevorzugt ist wenigstens eine mit der Analyseeinrichtung verbindbare Überwachungsreaktionseinrichtung zur Durchführung einer ersten Überwachungsreaktion vorgesehen. Die Analyseeinrichtung ist dann zum Ansteuern der Überwachungsreaktionseinrichtung ausgebildet, um eine erste Überwachungsreaktion in Abhängigkeit vom Ergebnis der Analyse der ersten Überwachungsdaten auszulösen.

- 30 Vorzugsweise ist als Überwachungsreaktionseinrichtung eine mit der Analyseeinrichtung verbindbare Abrechnungseinrichtung vorgesehen. Weiter vorzugsweise ist die Überwachungsreaktionseinrichtung zur Generierung von Betriebsbeeinflussungsdaten als erste Überwachungsreaktion ausgebildet, wobei Betriebsbeeinflussungsdaten die zur Beeinflus-

sung des Betriebs der ersten Einrichtung dienen. Die Datenzentrale ist dann zur Übertragung erster Daten an die erste Einrichtung ausgebildet, wobei die ersten Daten die Betriebsbeeinflussungsdaten umfassen. Schließlich weist die erste Einrichtung eine Betriebsbeeinflussungseinrichtung zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten auf.

Bei weiteren bevorzugten Varianten der erfindungsgemäßen Anordnung umfasst die erste Einrichtung eine erste Sicherheitseinrichtung, die zum Verifizieren der die Betriebsbeeinflussungsdaten umfassenden ersten Daten ausgebildet ist. Die Betriebsbeeinflussungseinrichtung ist dann zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit vom Ergebnis der Verifizierung ausgebildet.

Die vorliegende Erfindung betrifft weiterhin eine mobile erste Einrichtung, insbesondere Fahrzeug, für eine erfindungsgemäße Anordnung. Erfindungsgemäß umfasst die erste Einrichtung eine erste Datenübertragungseinrichtung zur Übertragung erster Daten und eine mit der ersten Datenübertragungseinrichtung verbindbare erste Sicherheitseinrichtung. Die Sicherheitseinrichtung ist zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet.

Bei einer bevorzugten Ausgestaltung der erfindungsgemäßen mobilen Einrichtung ist die erste Sicherheitseinrichtung zur Authentifizierung der ersten Datenübertragungseinrichtung ausgebildet. Hierzu ist sie bevorzugt zum Einbringen einer der ersten Datenübertragungseinrichtung zugeordneten Identifikation in den ersten Datensatz ausgebildet.

Die vorliegende Erfindung betrifft schließlich eine Datenzentrale für eine erfindungsgemäße Anordnung. Erfindungsgemäß weist die Datenzentrale eine Datenübertragungseinrichtung zur Übertragung erster Daten und eine mit der Datenübertragungseinrichtung verbindbare zweite Sicherheitseinrichtung auf, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

Um erhöhten Schutz vor unerkannter unbefugter Manipulation der gespeicherten ersten Daten, insbesondere der gespeicherten Erfassungswerte zu erzielen, ist die jeweilige Sicherheitseinrichtung bevorzugt zur Überprüfung der Zugriffsberechtigung auf wenigstens einen Teil der Sicherheitseinrichtung oder anderer Teile der ersten Einrichtung bzw. der Datenzentrale ausgebildet. Die Überprüfung kann sich dabei auf einzelne, entsprechend sicherheitsrelevante Bereiche der Sicherheitseinrichtung beschränken. Sie kann sich jedoch

auch auf die Überprüfung der Zugriffsberechtigung für sämtliche Bereiche der Sicherheitseinrichtung erstrecken.

Bevorzugt wird schon die Zugriffsberechtigung auf den Speicher überprüft, in dem die ersten Daten gespeichert sind, um den unberechtigten Zugriff auf die ersten Daten zu verhindern.

5 Es versteht sich jedoch, dass bei bestimmten Varianten der erfindungsgemäßen Anordnung der Zugriff auf den Speicher für die ersten Daten auch ohne besondere Zugriffsberechtigung zugelassen sein kann, wenn die ersten Daten bereits in entsprechend authentifizierter Weise gespeichert sind, dass nicht autorisierte Manipulationen an den ersten Daten erkennbar sind. Dies ist der Fall, wenn die ersten Daten beispielsweise bereits zusammen mit einer
10 unter Verwendung der ersten Daten erzeugten Authentifizierungsinformation, wie beispielsweise einem obengenannten MAC, einer digitalen Signatur oder dergleichen gespeichert sind. Die Authentifizierungsinformation wird dann bevorzugt, in einem Bereich der Sicherheitseinrichtung erzeugt, für den die Zugriffsberechtigung, sofern der Zugriff überhaupt möglich ist, überprüft wird.

15 Hierdurch wird erreicht, dass eine unbefugte Manipulation des gespeicherten ersten Daten zum einen entweder mangels Zugriff auf die ersten Daten überhaupt nicht möglich ist oder bei einer Überprüfung zumindest nicht unerkannt bleibt.

Die Überprüfung der Zugriffsberechtigung kann grundsätzlich in beliebiger geeigneter Weise erfolgen. So ist es beispielsweise möglich, ein Passwortsystem oder dergleichen zu implementieren. Bevorzugt ist vorgesehen, dass die Verarbeitungseinheit zur Überprüfung der
20 Zugriffsberechtigung unter Einsatz kryptographischer Mittel ausgebildet ist. Hierbei können beispielsweise digitale Signaturen und kryptographische Zertifikate zur Anwendung kommen. Dies ist von besonderem Vorteil, da derartige kryptographische Verfahren einen besonders hohen Sicherheitsstandard gewährleisten.

25 Hierbei können im übrigen wenigstens zwei unterschiedliche Zugriffsberechtigungsstufen vorgesehen sein, die mit unterschiedlichen Zugriffsrechten auf die Sicherheitseinrichtung bzw. mit ihr verbundenen Einrichtungen verknüpft sind. Hiermit lässt sich in einfacher Weise zum einen eine hierarchische Struktur mit unterschiedlich weit gehenden Zugriffsrechten implementieren. So kann beispielsweise dem Benutzer der Anordnung auf der untersten
30 Zugriffsberechtigungsstufe als einzige Zugriffshandlung erlaubt sein, die gespeicherten ersten Daten auszulesen, während einem Administrator auf einer höheren Zugriffsberechtigungsstufe neben dem Auslesen der ersten Daten gegebenenfalls die Modifikation weiterer Komponenten der Sicherheitseinrichtung etc. möglich ist.

Zum anderen lässt sich über die Zugriffsberechtigungsstufen auf derselben Hierarchieebene aber auch der Zugriff auf unterschiedliche Bereiche der Sicherheitseinrichtung bzw. mit ihr verbundenen Einrichtungen steuern. Die Anzahl der Zugriffsberechtigungsstufen oder Klassen richtet sich dabei nach der jeweiligen Verwendung der Anordnung und der Komplexität der mit der erfindungsgemäßen Anordnung realisierbaren Anwendungen.

Bei bevorzugten Ausgestaltungen der erfindungsgemäßen Anordnung werden die ersten Erfassungswerte verknüpft mit einer für den Erfassungszeitpunkt des ersten Erfassungswerts charakteristischen Erfassungszeitkennung ausgebildet. Durch diese häufig auch als Zeitstempel bezeichnete Verknüpfung des gespeicherten ersten Erfassungswerts mit dem Zeitpunkt seiner Erfassung wird die Weiterverarbeitung des Erfassungswerts, beispielsweise zu Zwecken der Abrechnung aber auch zu Zwecken der Statistik etc. deutlich erleichtert. Dies gilt insbesondere dann, wenn mehrere, zu unterschiedlichen Zeiten erfasste erste Erfassungswerte verarbeitet werden sollen.

Es versteht sich jedoch, dass es bei anderen Varianten der Erfindung ohne derartige Zeitstempel auch ausreichen kann, wenn lediglich durch geeignete Maßnahmen sichergestellt ist, dass die Chronologie der Erfassung der ersten Erfassungswerte nachvollziehbar ist. So können den ersten Erfassungswerten beispielsweise fortlaufende Nummern zugeordnet werden, um dieses Ziel zu erreichen.

Die Ermittlung der Erfassungszeit kann auf beliebige geeignete Weise erfolgen. Bevorzugt umfasst die Sicherheitseinrichtung zur Ermittlung der Erfassungszeitkennung ein mit der Verarbeitungseinheit verbundenes Zeiterfassungsmodul. Hierbei kann es sich um eine integrierte Echtzeituhr handeln oder ein Modul, das über eine geeignete Kommunikationsverbindung zu einer entsprechenden Instanz die Echtzeit abfragt. Die integrierte Echtzeituhr kann dabei gegebenenfalls von Zeit zu Zeit mit einer entsprechend genauen Zeitquelle synchronisiert werden.

Bei besonders günstigen Varianten der Erfindung ist wenigstens eine zweite Erfassungseinrichtung zur Erfassung wenigstens eines zweiten Erfassungswerts der ersten Erfassungsgröße vorgesehen. Mit diesen Varianten ist es möglich, auch größere Systeme mit mehreren Erfassungsorten der Erfassungsgröße, beispielsweise mehreren Messstellen für den Verbrauch eines Verbrauchsgutes, mit einer reduzierten Anzahl von Sicherheitseinrichtungen, gegebenenfalls sogar mit einer einzigen Sicherheitseinrichtung zu betreiben. Um die Trennung der ersten und zweiten Erfassungswerte sicherzustellen, kann vorgesehen sein, dass die ersten und zweiten Erfassungswerte in unterschiedlichen Speicherbereichen abgelegt

werden. Hierbei können insbesondere unterschiedliche Zugriffsberechtigungen für die unterschiedlichen Speicherbereiche definiert sein, um sicherzustellen, dass nur die jeweils autorisierten Personen bzw. Einrichtungen auf den entsprechenden Speicherbereich zugreifen können.

5 Besonders vorteilhaft ist es jedoch, wenn der erste Erfassungswert verknüpft mit einer für die erste Erfassungseinrichtung charakteristischen ersten Erfassungseinrichtungskennung und der zweite Erfassungswert verknüpft mit einer für die zweite Erfassungseinrichtung charakteristischen zweiten Erfassungseinrichtungskennung gespeichert wird. Mit dieser eindeutigen Zuordnung zwischen der Erfassungseinrichtung und dem durch sie erfassten Erfas-

10 sungswerts ist eine besonders einfache und zuverlässige Trennung möglich, welche die spätere Weiterverarbeitung erheblich erleichtert.

Bei weiteren günstigen Ausgestaltungen der erfindungsgemäßen Anordnung ist vorgesehen, dass die erste Erfassungseinrichtung zur Erfassung wenigstens eines dritten Erfassungswerts einer zweiten Erfassungsgröße ausgebildet ist. Alternativ kann eine dritte Erfassungsein-

15 einrichtung zur Erfassung wenigstens eines dritten Erfassungswerts einer zweiten Erfassungsgröße vorgesehen sein. Hierdurch ist es möglich, mit einer einzigen Sicherheitseinrichtung die Erfassung und gesicherte Speicherung der Erfassungswerte für unterschiedliche Erfassungsgrößen zu realisieren.

Um die Trennung der ersten und dritten Erfassungswerte sicherzustellen, kann auch hier

20 wieder vorgesehen sein, dass die ersten und dritten Erfassungswerte in unterschiedlichen Speicherbereichen abgelegt werden. Besonders vorteilhaft ist es jedoch auch hier, wenn der erste Erfassungswert verknüpft mit einer für die erste Erfassungsgröße charakteristischen ersten Erfassungsgrößenkennung und der dritte Erfassungswert verknüpft mit einer für die zweite Erfassungsgröße charakteristischen zweiten Erfassungsgrößenkennung gespeichert

25 wird. Mit dieser eindeutigen Zuordnung zwischen der Erfassungseinrichtung und der durch sie erfassten Erfassungsgröße ist eine besonders einfache und zuverlässige Trennung möglich, welche die spätere Weiterverarbeitung der gespeicherten Daten erheblich erleichtert.

Bei bevorzugten Varianten der erfindungsgemäßen Anordnung sind die erste Erfassungseinrichtung und die Sicherheitseinrichtung in einer vor unbefugtem Zugriff geschützten sicheren

30 Umgebung angeordnet, um in vorteilhafter Weise den unbefugten Zugriff nicht nur auf die Daten der Sicherheitseinrichtung sondern auch auf die Daten, die von und zu der ersten Erfassungseinrichtung geliefert werden, wirksam zu unterbinden.

Die sichere Umgebung kann dabei physisch durch ein oder mehrere entsprechend gesicherte Gehäuse hergestellt werden. Diese Gehäuse sind dann bevorzugt mit entsprechenden, hinlänglich bekannten Mitteln zur Erfassung von Manipulationen am Gehäuse ausgestattet. Bevorzugt erfolgt die Sicherung jedoch auch logisch durch ein entsprechend abgesichertes Kommunikationsprotokoll zwischen der ersten Erfassungseinrichtung und der Sicherheitseinrichtung. So kann beispielsweise vorgesehen sein, dass bei jeder Kommunikation zwischen der ersten Erfassungseinrichtung und der Sicherheitseinrichtung über eine entsprechend starke gegenseitige Authentifizierung ein gesicherter Kommunikationskanal aufgebaut wird. Es versteht sich, dass die erste Erfassungseinrichtung in diesem Fall über entsprechende Kommunikationsmittel verfügt, welche die beschriebene Sicherheitsfunktionalität zur Verfügung stellen.

Es versteht sich weiterhin, dass die sichere Umgebung durch solche logischen Sicherungsmechanismen auf einen beliebig großen Raum erstreckt werden kann. So können die erste Erfassungseinrichtung und die Sicherheitseinrichtung bei solchen Ausführungen innerhalb der sicheren Umgebung weit voneinander entfernt angeordnet sein. Es versteht sich weiterhin, dass die sichere Umgebung durch solche logischen Sicherungsmechanismen auch auf andere Komponenten, beispielsweise das Datenzentrum, ausgeweitet werden kann.

Es versteht sich, dass sämtliche der oben beschriebenen Module und Funktionen der Sicherheitseinrichtung durch entsprechend gestaltete Hardwaremodule realisiert sein können. Bevorzugt sind sie jedoch zumindest zum Teil als Softwaremodule gestaltet, auf welche die Verarbeitungseinheit zugreift, um die entsprechende Funktion zu realisieren. Weiterhin versteht es sich, dass die einzelnen Speicher nicht durch getrennte Speichermodule realisiert sein müssen. Vielmehr handelt es sich bevorzugt um entsprechend logisch getrennte Speicherbereiche eines einzigen Speichers, beispielsweise eines einzigen Speichermoduls.

Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen bzw. der nachstehenden Beschreibung eines bevorzugten Ausführungsbeispiels, welche auf die beigefügten Zeichnungen Bezug nimmt. Es zeigen

Figur 1 eine schematische Darstellung einer bevorzugten Ausführungsform der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens;

Figur 2 ein Blockschaltbild von Komponenten der Anordnung aus Figur 1;

Figur 3 eine schematische Darstellung einer weiteren bevorzugten Ausführungsform der erfindungsgemäßen Anordnung;

Figur 4 eine schematische Darstellung einer weiteren bevorzugten Ausführungsform der erfindungsgemäßen Anordnung.

5 Figur 1 zeigt ein bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung zur Durchführung des erfindungsgemäßen Verfahrens zur Übertragung von Daten zwischen einer mobilen ersten Einrichtung in Form eines Fahrzeugs 1 und einer davon entfernten Datenzentrale 2. Bei dem Fahrzeug 1 handelt es sich im vorliegenden Beispiel um einen Mietwagen. Die vorliegende Erfindung wird hierbei im Zusammenhang mit der Überwachung
10 und insbesondere mit der Abrechnung für die Nutzung dieses Mietwagens eingesetzt.

Das Fahrzeug 1 umfasst eine mobile erste Übertragungseinrichtung in Form eines ersten Mobilfunkmoduls 1.1 für ein Mobilfunknetz 3. Mittels des Mobilfunkmoduls 1.1 können Daten über eine zweite Übertragungseinrichtung 3.1 des Mobilfunknetzes 3 mit einer dritten Übertragungseinrichtung in Form eines zweiten Mobilfunkmoduls 2.1 der Datenzentrale 2 aus-
15 getauscht werden.

Das Fahrzeug 1 weist weiterhin eine mit dem ersten Mobilfunkmodul 1.1 verbundene erste Sicherheitseinrichtung in Form eines ersten Sicherheitsmoduls 1.2 auf. Spätestens wenn über das Mobilfunknetz 3 sicherheitsrelevante Daten von dem Fahrzeug 1 zur Datenzentrale 2 übertragen werden sollen, generiert das erste Sicherheitsmodul 1.2 einen erste Daten dar-
20 stellenden ersten Datensatz, der unter anderem die zu übertragenden sicherheitsrelevanten Daten umfasst. Anschließend authentifiziert das erste Sicherheitsmodul 1.2 die ersten Daten unter Verwendung kryptographischer Mittel.

Hierzu ordnet das erste Sicherheitsmodul 1.2 dem ersten Datensatz eine Authentifizierungsinformation zu, indem es zunächst unter Verwendung eines entsprechenden kryptographischen Algorithmus und eines privaten ersten kryptographischen Schlüssels des Si-
25 cherheitsmoduls 1.2 über dem ersten Datensatz eine erste digitale Signatur als Authentifizierungsinformation bildet. Anschließend bildet das Sicherheitsmodul 1.2 aus dem ersten Datensatz und der ersten digitalen Signatur einen zweiten Datensatz.

Die erste digitale Signatur, also die Authentifizierungsinformation, stellt sicher, dass zu ei-
30 nem späteren Zeitpunkt durch eine Verifikation der ersten digitalen Signatur zweifelsfrei festgestellt werden kann, ob der erste Datensatz und damit die ersten Daten manipuliert wurden oder ob es sich nach wie vor um authentische Daten handelt.

Um die Sicherheit vor unbefugtem Zugriff auf die Daten zu erhöhen, verschlüsselt das erste Sicherheitsmodul 1.2 den zweiten Datensatz unter Verwendung eines zweiten kryptographischen Schlüssels, wobei ein dritter Datensatz entsteht. Dieser dritte Datensatz wird von dem ersten Sicherheitsmodul 1.2 an das erste Mobilfunkmodul 1.1 übergeben. Das erste Mobilfunkmodul 1.1 überträgt den dritten Datensatz dann über das Mobilfunknetz 3 an das zweite Mobilfunkmodul 2.1 der Datenzentrale 2.

Das zweite Mobilfunkmodul 2.1 gibt den dritten Datensatz an eine damit verbundene zweite Sicherheitseinrichtung in Form eines zweiten Sicherheitsmoduls 2.2 weiter. Das zweite Sicherheitsmodul 2.2 entschlüsselt den und dritten Datensatz unter Verwendung eines dritten kryptographischen Schlüssels, um so wieder den zweiten Datensatz zu erhalten. Der dritte Schlüssel entspricht dabei dem zweiten Schlüssel. Es handelt sich hierbei im vorliegenden Fall um einen zuvor ausschließlich für diese Übertragungssitzung generierten geheimen Sitzungsschlüssel. Dieser wurde zuvor separat in dem ersten Sicherheitsmodul 1.2 und dem zweiten Sicherheitsmodul 2.2 generiert. Die Generierung und Verwendung solcher geheimer einmalig verwendeter Sitzungsschlüssel ist an sich bekannt, sodass hierauf an dieser Stelle nicht näher eingegangen werden soll.

Es versteht sich jedoch, dass bei anderen Varianten der Erfindung, sofern eine solche Absicherung erforderlich ist, auch ein anderer Absicherungsmechanismus gewählt werden kann. Insbesondere kann bei Verwendung einer asymmetrischen Verschlüsselung der zweite kryptographische Schlüssel beispielsweise ein öffentlicher Schlüssel des zweiten Sicherheitsmoduls sein. Der dritte Schlüssel ist dann entsprechend der zugehörige private Schlüssel des zweiten Sicherheitsmoduls.

Aus dem zweiten Datensatz extrahiert das zweite Sicherheitsmodul 2.2 den ersten Datensatz und die erste digitale Signatur. Anhand des ersten Datensatzes und eines dem ersten kryptographischen Schlüssel zugeordneten vierten kryptographischen Schlüssels verifiziert das zweite Sicherheitsmodul 2.2 dann in an sich bekannter Weise die erste digitale Signatur, um die Authentizität des ersten Datensatzes und damit der ersten Daten festzustellen.

Derselbe Ablauf ergibt sich in der anderen Richtung, wenn sicherheitsrelevante Daten von der Datenzentrale 2 an das Fahrzeug 1 übermittelt werden sollen. Hierbei führt das zweite Sicherheitsmodul 2.2 dann die oben für das erste Sicherheitsmodul 1.2 beschriebenen Operationen durch und umgekehrt.

Im Rahmen der Kommunikation zwischen dem Fahrzeug 1 und der Datenzentrale 2 findet eine starke wechselseitige Authentifizierung der Kommunikationspartner unter Einsatz ent-

sprechender kryptographischer Mittel statt, wobei insbesondere entsprechende kryptographische Zertifikate Verwendung finden. Dies geschieht wiederum unter Verwendung des ersten Sicherheitsmoduls 1.2 und des zweiten Sicherheitsmoduls 2.2. Verfahren für eine solche starke wechselseitige Authentifizierung der Kommunikationspartner sind hinlänglich bekannt, sodass hierauf nicht näher eingegangen werden soll.

Figur 2 zeigt ein Blockschaltbild von Komponenten des Fahrzeugs 1. Wie dieser Figur zu entnehmen ist, weist das erste Sicherheitsmodul 1.2 eine erste Verarbeitungseinheit 1.3 auf, die mit dem ersten Mobilfunkmodul 1.1 verbunden ist. Mit der ersten Verarbeitungseinheit 1.3 ist weiterhin ein Kryptographiemodul 1.4 verbunden, welches die oben beschriebenen kryptographischen Mittel zur Verfügung stellt und hierzu entsprechende Kryptographiedaten enthält. Die Kryptographiedaten umfassen unter anderem kryptographischen Algorithmen und entsprechende kryptographische Schlüssel. Neben den kryptographischen Algorithmen und Schlüsseln umfassen die Kryptographiedaten des Kryptographiemoduls 1.4 weitere Daten, wie beispielsweise ein oder mehrere kryptographische Zertifikate entsprechender Zertifizierungsinstanzen sowie gegebenenfalls ein oder mehrere eigene kryptographische Zertifikate der Sicherheitseinrichtung 1.2.

Das Sicherheitsmodul 1.2 ist zum Austausch wenigstens eines Teils der Kryptographiedaten ausgebildet, um eine einfache und dauerhaft zuverlässige Sicherung der Daten zu gewährleisten. Hierbei ist vorgesehen, dass neben den kryptographischen Schlüsseln und kryptographischen Zertifikaten auch der jeweils verwendete kryptographische Algorithmus ausgetauscht werden kann, um das System an geänderte Sicherheitsanforderungen anpassen zu können. Die Implementierung und der Austausch der Kryptographiedaten erfolgt im Rahmen einer so genannten Public Key Infrastruktur (PKI), wie sie hinlänglich bekannt ist und daher an dieser Stelle nicht weiter beschrieben werden soll. Es versteht sich insbesondere, dass eine entsprechende Routine zur Überprüfung der Validität der verwendeten kryptographischen Zertifikate vorgesehen ist. Geeignete derartige Überprüfungsroutinen sind ebenfalls hinlänglich bekannt und sollen daher hier nicht näher beschrieben werden.

Das Kryptographiemodul 1.4 wird sowohl zur Verschlüsselung zu speichernder Daten verwendet werden als auch zur Verschlüsselung zu übertragender Daten. Es versteht sich, dass je nach Anwendung, also beispielsweise je nachdem, ob Daten versandt oder gespeichert werden sollen, auch unterschiedliche kryptographische Verfahren angewendet werden können.

Nach der erfolgreichen Übertragung des dritten Datensatzes erstellt das erste Sicherheitsmodul 1.2 einen Protokolldatensatz, den es in einem mit der ersten Verarbeitungseinheit 1.3 verbundenen ersten Protokollspeicher 1.5 ablegt. Der Protokolldatensatz umfasst den ersten Datensatz sowie die über dem ersten Datensatz in der oben beschriebenen Weise erstellte
5 erste digitale Signatur. Der umfasst mit anderen Worten also die authentifizierten ersten Daten. Der erste Protokollspeicher 1.5 kann dabei so gestaltet sein, dass der Protokolldatensatz lediglich gelesen aber nicht verändert werden kann. Weiterhin kann der erste Protokollspeicher 1.5 so dimensioniert sein, dass er sämtliche über die Lebensdauer des ersten Sicherheitsmoduls 1.2 oder des Fahrzeugs 1 zu erwartenden Protokolldatensätze aufnehmen kann.
10

Im vorliegenden Beispiel werden die Protokolldatensätze im Klartext gespeichert. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung vorgesehen sein kann, dass die Protokolldatensätze in verschlüsselter Form gespeichert werden können, um sie vor unbefugter Einsicht zu schützen.

15 Im Folgenden wird unter Bezugnahme auf die Figuren 1 und 2 die Generierung der an die Datenzentrale 2 zu übertragenden sicherheitsrelevanten ersten Daten näher beschrieben.

Die ersten Daten umfassen zum einen erste Erfassungswerte einer ersten Erfassungsgröße, die durch eine mit der ersten Verarbeitungseinheit 1.3 verbundene erste Erfassungseinrichtung 4 erfasst wurden. Bei den ersten Erfassungswerten handelt es sich um die aktuellen
20 Werte des Kilometerstands des Fahrzeugs 1 als erster Erfassungsgröße. Diese Kilometerwerte werden von dem Kilometerzähler 4 des Fahrzeugs 1 als erster Erfassungseinrichtung erfasst und zu vorgegebenen Zeiten, beispielsweise in regelmäßigen Abständen, an die erste Verarbeitungseinheit 1.3 weitergegeben.

Die erste Verarbeitungseinheit 1.3 verknüpft diese Kilometerwerte mit einer für den Zeitpunkt
25 ihrer Erfassung charakteristischen Erfassungszeitkennung, einem so genannten Zeitstempel, indem sie den Kilometerwert und die Erfassungszeitkennung in einen ersten Kilometerdatensatz schreibt. Hierzu greift sie auf ein Zeiterfassungsmodul 1.6 des ersten Sicherheitsmoduls 1.2 zu, welches eine entsprechend zuverlässige Zeitinformation liefert. Bei dem Zeiterfassungsmodul handelt es sich um eine integrierte Echtzeituhr, die von Zeit zu Zeit mit
30 einer entsprechend genauen Zeitquelle synchronisiert wird. Es versteht sich, dass es sich bei anderen Varianten der Erfindung ebenso um ein Modul handeln kann, das über eine geeignete Kommunikationsverbindung zu einer entsprechenden Instanz die Echtzeit abfragt.

Die erste Verarbeitungseinheit 1.3 verknüpft die Kilometerwerte weiterhin mit einer für den Kilometerzähler 4 charakteristischen ersten Erfassungseinrichtungskennung, indem sie diese ebenfalls in den ersten Kilometerdatensatz schreibt. Hierbei handelt es sich um eine für den betreffenden Kilometerzähler 4 einmalige und eindeutige Identifikation, die gleichzeitig eine erste Quellenidentifikation für die Quelle der Kilometerwerte darstellt. Die erste Erfassungseinrichtungskennung stellt gleichzeitig eine erste Erfassungsgrößenkennung dar, da der Kilometerzähler 4 ausschließlich Kilometerwerte liefert. Es versteht sich, dass bei anderen Erfassungseinrichtungen, die unterschiedliche Erfassungsgrößen erfassen, den jeweiligen Erfassungswerten gegebenenfalls mit einer entsprechenden Erfassungsgrößenkennung verknüpft werden können.

Es versteht sich, dass die vorgenannte Verknüpfung der Kilometerwerte mit der Erfassungszeitkennung und der Erfassungseinrichtungskennung durch kryptographische Mittel abgesichert werden kann. So kann beispielsweise vorgesehen sein, dass das erste Sicherheitsmodul 1.2 eine zweite digitale Signatur über diesen Daten erstellt, sodass diese durch die ihnen dann beigefügte zweite digitale Signatur ebenfalls manipulationssichere miteinander verknüpft sind. Ebenso kann natürlich für beliebige andere einander zugeordnete Daten verfahren werden, um diese manipulationssicher miteinander zu verknüpfen.

Der so generierte erste Kilometerdatensatz wird dann von der ersten Verarbeitungseinheit 1.3 in einem mit ihr verbundenen ersten Speicher 1.7 abgelegt.

Die ersten Daten umfassen weiterhin zweite Erfassungswerte einer zweiten Erfassungsgröße und dritte Erfassungswerte einer dritten Erfassungsgröße, die durch eine mit der ersten Verarbeitungseinheit 1.3 verbundene zweite Erfassungseinrichtung 5 erfasst wurden. Bei den zweiten Erfassungswerten handelt es sich um die aktuellen Werte des Motorölstands des Fahrzeugs 1 als zweiter Erfassungsgröße. Bei dritten Erfassungswerten handelt es sich um die aktuellen Werte der Bremsenqualität des Fahrzeugs 1 als dritter Erfassungsgröße. Diese Bremsenqualitätswerte werden von der Fahrzeugüberwachungseinrichtung 5 des Fahrzeugs 1 als zweiter Erfassungseinrichtung erfasst und ebenfalls zu vorgegebenen Zeiten, beispielsweise in regelmäßigen Abständen, an die erste Verarbeitungseinheit 1.3 weitergegeben.

Die erste Verarbeitungseinheit 1.3 verknüpft diese zweiten und dritten Erfassungswerte mit einer für den Zeitpunkt ihrer Erfassung charakteristischen Erfassungszeitkennung, indem sie den Motorölstandswert, den Bremsenqualitätswert und die Erfassungszeitkennung in einen

ersten Fahrzeugzustandsdatensatz schreibt. Hierzu greift sie auf ein Zeiterfassungsmodul 1.6 der ersten Sicherheitseinrichtung 1.2 zu.

Die erste Verarbeitungseinheit 1.3 verknüpft die Motorölstandswerte und die Bremsenqualitätswerte weiterhin mit einer für die Fahrzeugüberwachungseinrichtung 5 charakteristischen zweiten Erfassungseinrichtungskennung, indem sie diese ebenfalls in den ersten Fahrzeugzustandsdatensatz schreibt. Hierbei handelt es sich um eine für die betreffende Fahrzeugüberwachungseinrichtung 5 einmalige und eindeutige Identifikation, die gleichzeitig eine zweite Quellenidentifikation für die Quelle der Motorölstandswerte und Bremsenqualitätswerte darstellt. Weiterhin wird den jeweiligen Erfassungswerten eine entsprechenden Erfassungsgrößenkennung zugeordnet, indem diese entsprechend zugeordnet mit in den Fahrzeugzustandsdatensatz geschrieben wird.

Der so generierte erste Fahrzeugzustandsdatensatz wird dann von der ersten Verarbeitungseinheit 1.3 ebenfalls in dem ersten Speicher 1.7 abgelegt.

Zu einem bestimmten vorgegebenen oder wählbaren Zeitpunkt sollen dann die zwischenzeitlich im ersten Speicher 1.7 abgelegten Kilometerdatensätze und Fahrzeugzustandsdatensätze als erste Überwachungsdaten an die Datenzentrale 2 übertragen werden. Die erste Verarbeitungseinheit 1.3 liest hierzu die gespeicherten Kilometerdatensätze und Fahrzeugzustandsdatensätze aus dem ersten Speicher 1.7 aus und schreibt sie in den ersten Datensatz.

Die erste Verarbeitungseinheit 1.3 ergänzt den ersten Datensatz weiterhin um eine dem ersten Sicherheitsmodul 1.2 zugeordnete einmalige und eindeutige erste Sicherheitsmodulidentifikation sowie um einen unter Zugriff auf das erste Zeiterfassungsmodul 1.6 generierten ersten Zeitstempel. Die erste Sicherheitsmodulidentifikation stellt dabei eine dritte Quellenidentifikation dar, während der erste Zeitstempel den Zeitpunkt der Zusammenstellung der ersten Überwachungsdaten charakterisiert. Weiterhin ergänzt die erste Verarbeitungseinheit 1.3 den ersten Datensatz um eine einmalige und eindeutige Identifikation des ersten Mobilfunkmoduls 1.1, die ebenfalls als Quellenidentifikation dient.

Schließlich ergänzt die erste Verarbeitung einer 1.3 den ersten Datensatz um eine Übertragungsidentifikation in Form einer fortlaufenden Transaktionsnummer, die dem laufenden Übertragungsvorgang eindeutig zugeordnet ist.

Anschließend wird der erste Datensatz in der oben beschriebenen Weise authentifiziert und in Form des dritten Datensatzes an die Datenzentrale 2 übertragen.

Sobald die Datenzentrale 2 die Authentizität des ersten Datensatzes überprüft hat, sendet sie einen entsprechenden Bestätigungsdatensatz an das Fahrzeug 1. Dieser Bestätigungsdatensatz umfasst eine dem zweiten Sicherheitsmodul zugeordnete zweiten Sicherheitsmodulidentifikation. Die zweite Sicherheitsmodulidentifikation stellt dabei eine erste Empfängeridentifikation dar, die den Empfänger des ersten Datensatzes kennzeichnet.

Die erste Verarbeitungseinheit 1.3 schreibt diesen Bestätigungsdatensatz zusammen mit einem für den Zeitpunkt des Erhalts des Bestätigungsdatensatzes charakteristischen zweiten Zeitstempel in den vorhandenen ersten Datensatz und authentifiziert diesen dann wieder in der oben beschriebenen Weise, indem sie eine digitale Signatur über dem ersten Datensatz bildet. Diese digitale Signatur wird dann zusammen mit dem ersten Datensatzes in einen ersten Protokolldatensatz geschrieben, der dann in der oben beschriebenen Weise in den ersten Protokollspeicher 1.5 eingebracht wird.

Der erste Protokolldatensatz wird anschließend an die Datenzentrale 2 übermittelt, wo er nach entsprechender Überprüfung seiner Authentizität in einem mit dem zweiten Sicherheitsmodul 2.2 verbundenen zweiten Protokollspeicher 2.3 gespeichert wird. Es versteht sich, dass die Datenzentrale 2 bei anderen Varianten der Erfindung auch einen solchen Protokolldatensatz selbst generieren und in den zweiten Protokollspeicher ablegen kann.

Dieser erste Protokolldatensatz authentifiziert somit in vorteilhafter Weise sowohl die Quellen und den Empfänger der jeweiligen Daten, bestimmte Erfassungs- und Verarbeitungszeitpunkte sowie die Übertragung selbst, sodass die mit diesen Daten verbundenen Sachverhalte zu einem späteren Zeitpunkt zweifelsfrei nachgewiesen werden können. Insbesondere ist es möglich, den Empfang der ersten Daten in der Datenzentrale 2 nachzuweisen.

Nach Erhalt und Überprüfung der Authentizität der ersten Daten in der Datenzentrale 2 werden diese alleine mit dem Sicherheitsmodul 2.2 verbundene Analyseeinrichtung 2.4 der Datenzentrale 2 übermittelt. Diese analysiert die übermittelten ersten Daten. Hierbei berücksichtigt die unter anderem statistische Daten, welche nicht von dem Fahrzeug 1 stammen.

Die Analyseeinrichtung 2.4 löst zum einen in Abhängigkeit von den übermittelten Kilometerwerten als erste Überwachungsreaktion einen ersten Abrechnungsvorgang für die gefahrenen Kilometer durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene Abrechnungsmodule 2.5 als erster Überwachungsreaktionseinrichtung aus.

Als zweite Überwachungsreaktion löst die Analyseeinrichtung 2.4 in Abhängigkeit von der Analyse der ersten Daten die Generierung von Betriebsbeeinflussungsdaten für das Fahr-

zeug 1 durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene zweite Überwachungsreaktionseinrichtung 2.6 aus. Diese Betriebsbeeinflussungsdaten werden in einem weiteren ersten Datensatz von der Datenzentrale 2 über das Mobilfunknetz 3 an das Fahrzeug 1 übermittelt. Hierbei wird analog zu der oben beschriebenen Übermittlung der ersten Daten
5 von dem Fahrzeug 1 zu Datenzentrale 2 verfahren, sodass diesbezüglich auf die obigen Ausführungen verwiesen wird. Insbesondere werden die ersten Daten in analoger Weise authentifiziert und es wird ein entsprechender Protokolldatensatz für die Übertragung generiert und sowohl im Fahrzeug 1 als auch in der Datenzentrale 2 gespeichert.

Die Betriebsbeeinflussungsdaten umfassen zum einen in Abhängigkeit von den übermittelten Kilometerwerten einen Hinweis über die aktuell gefahrenen Kilometer, den hierfür aktuellen Tarif sowie den aktuellen Abrechnungswert. Dieser Hinweis wird nach Verifizierung der Authentizität der Betriebsbeeinflussungsdaten im ersten Sicherheitsmodul 1.2 an eine mit dem ersten Sicherheitsmodul 1.2 verbundene Betriebsbeeinflussungseinrichtung 6 weitergegeben, welche diesen wiederum über ein damit verbundenes Display 7 an den Nutzer des
10 Fahrzeugs 1 ausgibt. Die Betriebsbeeinflussungsdaten können weiterhin in Abhängigkeit von der Analyse der übermittelten Fahrzeugüberwachungsdaten (Motorölstand und Bremsenqualität) im Falle des Drohens kritischer Zustände entsprechende Warnhinweise enthalten, die ebenfalls über das Display 7 an den Nutzer des Fahrzeugs 1 ausgegeben werden.

Schließlich löst die Analyseeinrichtung 2.4 als dritte Überwachungsreaktion in Abhängigkeit von der Analyse der ersten Daten die Durchführung eines Wartungsprotokolls für das Fahrzeug 1 durch eine mit dem zweiten Sicherheitsmodul 2.2 verbundene dritte Überwachungsreaktionseinrichtung in Form einer Fahrzeugmanagementsseinrichtung 2.7 aus. Hierbei kann in Abhängigkeit von den Überwachungsdaten unter anderem die Wartung des Fahrzeuges 1 bei Rückgabe geplant und vorbereitet werden. Insbesondere können erforderliche Ersatzteile oder dergleichen bereits vorab bestellt werden, um die erforderliche Zeit für die Wartung so kurz wie möglich zu halten und damit die Ausfallzeiten des Fahrzeugs 1 zu verringern.
20

Die Erfassungseinrichtungen 4 und 5, das erste Sicherheitsmodul 1.2 und das erste Mobilfunkmodul 1.1 sind in einer vor unbefugtem Zugriff geschützten sicheren Umgebung 1.3 angeordnet, um den unbefugten Zugriff nicht nur auf die Daten des Sicherheitsmoduls ein
30 vom zweiten sondern auch auf die Daten, die von und zu den Erfassungseinrichtungen 4 und 5 bzw. dem ersten Mobilfunkmodul 1.1 geliefert werden, wirksam zu unterbinden.

Die sichere Umgebung 1.3 wird zum einen physisch durch sichere Gehäuse der Erfassungseinrichtungen 4 und 5, des Mobilfunkmoduls 1.1 und des ersten Sicherheitsmoduls 1.2 hergestellt, die mit hinlänglich bekannten Mittel zur Erfassung von Manipulationen am Gehäuse ausgestattet sind. Zum anderen wird sie logisch durch ein entsprechend abgesichertes Kommunikationsprotokoll zwischen diesen Komponenten hergestellt. So wird bei jeder Kommunikation zwischen diesen Komponenten über eine entsprechend starke gegenseitige Authentifizierung ein gesicherter Kommunikationskanal aufgebaut. Es versteht sich, dass die Komponenten hierzu über entsprechende Kommunikationsmittel verfügen, welche die beschriebenen Sicherheitsfunktionalitäten zur Verfügung stellen.

Es versteht sich jedoch, dass bei anderen Varianten der Erfindung je nach den zu stellenden Sicherheitsanforderungen keine oder lediglich einzelne der genannten Komponenten in einer entsprechenden sicheren Umgebung angeordnet sein können.

Figur 3 zeigt ein weiteres bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung, die in ihrer grundsätzlichen Funktion derjenigen aus Figur 1 gleicht, sodass hier lediglich auf die Unterschiede eingegangen werden soll.

Ein Unterschied besteht darin, dass es sich bei der mit dem ersten Sicherheitsmodul 1.2' verbundenen ersten Übertragungseinrichtung des Fahrzeugs 1' um eine kurzreichweitige erste Infrarotschnittstelle 1.1' handelt. Die Infrarotschnittstelle 1.1' arbeitet dabei nach dem IrDA-Standard. Es versteht sich jedoch, dass bei anderen Varianten der Erfindung auch beliebige andere Übertragungsverfahren mit kurzer Reichweite, wie beispielsweise Bluetooth etc., verwendet werden können.

Die zweite Übertragungseinrichtung ist von einem Serviceterminal 8 gebildet. Dieses Serviceterminal 8 umfasst eine entsprechende zweite Infrarotschnittstelle 8.1 und ein damit verbundenes Kommunikationsmodul 8.2, welches die von der zweiten Infrarotschnittstelle 8.1 empfangenen ersten Daten über ein Telekommunikationsnetz 9 an die Datenzentrale 2' übermittelt.

Die Generierung, Authentifizierung, Übermittlung und Protokollierung der sicherheitsrelevanten ersten Daten von dem Fahrzeug 1' zur Datenzentrale 2' und umgekehrt erfolgt analog der oben in Zusammenhang mit Figur 1 beschriebenen Ausführungsform, sodass hier lediglich auf die obigen Ausführungen verwiesen wird.

Ein weiterer Unterschied besteht darin, dass das erste Sicherheitsmodul 1.2' mit einer Fahrzeugmanagementüberwachungseinrichtung 10 verbunden ist, die wiederum mit der Fahr-

zeugmanagementeinrichtung 11 des Fahrzeugs 1' verbunden ist. Die Fahrzeugmanagementeinrichtung 11 stellt dabei diejenige Einrichtung dar, welche die Funktionen der einzelnen Komponenten des Fahrzeugs steuert. Sie umfasst insbesondere das Motormanagement etc.

- 5 Die Fahrzeugmanagementüberwachungseinrichtung 10 überwacht in diesem Fall als dritte Erfassungseinrichtung unter anderem die Funktion der Softwarekomponenten der Fahrzeugmanagementeinrichtung 11. Die von der Fahrzeugmanagementüberwachungseinrichtung 10 erfassten Daten werden als dritte Erfassungswerte und damit als Überwachungsdaten in der oben beschriebenen Weise in einen ersten Datensatz eingebracht, authentifiziert und an die Datenzentrale 2' übermittelt.

- In Abhängigkeit von der Analyse der übermittelten Überwachungsdaten in der Datenzentrale 2' generiert, authentifiziert und sendet die Datenzentrale 2' entsprechende Betriebsbeeinflussungsdaten in der oben beschriebenen Weise über das Serviceterminal 8 an das Fahrzeug 1'. Bei der Analyse der Überwachungsdaten überprüft die Datenzentrale 2' nicht nur die
- 15 Integrität der Fahrzeugmanagementeinrichtung 11. Sie überprüft unter anderem auch die aktuelle Version der durch die Fahrzeugmanagementeinrichtung 11 verwendeten Softwaremodule. Existiert für eines der Softwaremodule eine neue Version, wird diese als Bestandteil der Betriebsbeeinflussungsdaten an das Fahrzeug 1' übersandt.

- Nach dem das erste Sicherheitsmodul 1.2' die Authentizität der Betriebsbeeinflussungsdaten
- 20 in der oben beschriebenen Weise verifiziert hat, gibt es die Betriebsbeeinflussungsdaten, insbesondere das neue Softwaremodul an die Fahrzeugmanagementüberwachungseinrichtung 10 weiter. Diese Fahrzeugmanagementüberwachungseinrichtung 10 stellt gleichzeitig eine Betriebsbeeinflussungseinrichtung dar, indem sie den Austausch des nichtmehr aktuellen alten Softwaremoduls durch das neue Softwaremodul in der Fahrzeugmanagementeinrichtung 11 steuert.

- Auch die Übertragung der Betriebsbeeinflussungsdaten von der Datenzentrale 2' zum Fahrzeug 1 wird in der oben beschriebenen Weise protokolliert. Hierbei wird in den entsprechenden ersten Datensatz zudem eine Identifikation des Serviceterminals 8 als Quellenidentifikation aufgenommen, um auch die Übertragung über dieses Serviceterminal 8 zu einem späteren zweifelsfrei nachvollziehen zu können.

Insbesondere wird hier die Identifikation des ersten Sicherheitsmoduls 1.2' als Empfängeridentifikation in den ersten Datensatz des Protokolldatensatzes aufgenommen. Dies kann in Fällen, in denen der Austausch des betreffenden Softwaremoduls kostenpflichtig ist, später

als Nachweis dienen, dass der Softwaremodul tatsächlich im Fahrzeug 1' empfangen wurde. Gegebenenfalls kann auch eine entsprechende Austauschbetätigung in den ersten Datensatz aufgenommen werden, um auch den tatsächlichen Austausch zweifelsfrei nachvollziehbar zu machen.

- 5 Es versteht sich, dass in solchen Fällen eines kostenpflichtigen Wartung der Fahrzeugsoftware oder auch bei anderen kostenpflichtigen Betriebsbeeinflussungen in der Datenzentrale mit Erhalt einer entsprechenden Empfangsbestätigung vom Fahrzeug 1' ein entsprechender Abrechnungsvorgang ausgelöst werden kann.

- 10 Die Kommunikation zwischen dem Fahrzeug 1' und der Datenzentrale 2' läuft wie die oben im Zusammenhang mit Figur 1 beschriebene Kommunikation ab. Insbesondere findet jeweils eine starke wechselseitige Authentifizierung unter Verwendung kryptographischer Mittel statt, sodass in Verbindung mit der Authentifizierung der ersten Daten jeweils gewährleistet ist, dass nur autorisierte und authentische Daten ausgetauscht und verwendet werden.

- 15 Mit dem beschriebenen Ausführungsbeispiel lässt sich beispielsweise ein flächendeckendes Netz von Serviceterminals 8 realisieren, über das eine einfache Überwachung und Fernwartung von Fahrzeugen möglich ist.

- 20 Das Ausführungsbeispiel wurde vorstehend anhand einer drahtlosen Verbindung zum Serviceterminal 8 beschrieben. Es versteht sich jedoch, dass bei anderen Varianten auch eine drahtgebundene Verbindung zum Serviceterminal vorgesehen sein kann, wie dies in Figur 3 durch den Pfeil 12 angedeutet ist. So kann beispielsweise ein Datenkabel verwendet werden, welches das Fahrzeug über entsprechende serielle Schnittstellen mit der zweiten Übertragungseinrichtung des Serviceterminals verbindet.

- 25 Weiterhin versteht es sich, dass es sich bei anderen Varianten der Erfindung bei dem Serviceterminal ebenfalls um eine mobile Einrichtung handeln kann, die dann gegebenenfalls über ein Mobilfunknetz oder dergleichen eine Verbindung zur Datenzentrale herstellt. Eine derartige Variante der Erfindung eignet sich besonders für den Einsatz in Zusammenhang mit Pannendiensten oder dergleichen.

- 30 Schließlich versteht es sich, dass das erste Sicherheitsmodul nicht notwendigerweise Bestandteil der mobilen Einheit sein muss. So ist es im Zusammenhang mit den soeben genannten Serviceterminals, insbesondere den mobilen Serviceterminals, möglich, das erste Sicherheitsmodul oder Teile davon, beispielsweise das Kryptographiemodul, in dem Serviceterminal zu integrieren. Dabei kann dann vorgesehen sein, dass die mobile Einrichtung

beispielsweise neben den Erfassungseinrichtungen sowie einer entsprechenden Schnittstelle zur Verbindung mit dem Serviceterminal lediglich den ersten Protokollspeicher aufweist, in den der Protokolldatensatz durch das Serviceterminal geschrieben wird.

5 Figur 4 zeigt ein weiteres bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Anordnung, die in ihrer grundsätzlichen Funktion derjenigen aus Figur 1 gleicht, sodass hier lediglich auf die Unterschiede eingegangen werden soll.

Ein Unterschied besteht darin, dass das erste Sicherheitsmodul 1.2" eines Lastkraftwagens als erstem Fahrzeug 1" über einen Fahrzeugdatenbus 13 nicht nur mit einer Erfassungseinrichtung 14 des Fahrzeugs 1" verbunden ist, über die Zustandsdaten des Fahrzeugs, unter
10 anderem dessen Position, ermittelt werden. Vielmehr ist das erste Sicherheitsmodul 1.2" auch mit einer Erfassungseinrichtung 15.1 eines geladenen ersten Containers 15 und einer Erfassungseinrichtung 16.1 eines geladenen zweiten Containers 16 verbunden. Über die Erfassungseinrichtungen 15.1 und 16.1 werden jeweils Zustandsdaten des Containers 15 bzw. 16 und seiner Ladung erfasst.

15 Bei dem Fahrzeugdatenbus 13 handelt es sich im vorliegenden Fall um einen drahtlosen Datenbus. Es versteht sich jedoch, dass bei anderen Varianten der vorliegenden Erfindung auch ein drahtgebundener Datenbus verwendet werden kann.

Die Erfassungswerte der Erfassungseinrichtungen 14, 15.1 und 16.1 werden an das erste Sicherheitsmodul 1.2" weitergegeben und dann in der oben in Zusammenhang mit Figur 1
20 beschriebenen Weise über ein mit dem ersten Sicherheitsmodul 1.2" verbundenes erstes Mobilfunkmodul an eine - nicht dargestellte - entfernte Datenzentrale übermittelt.

Hiermit ist es nicht nur möglich, den Zustand des Fahrzeugs 1" zu überwachen und gegebenenfalls zu beeinflussen. Vielmehr ist es mit einem einzigen Sicherheitsmodul 1.2" auch möglich, den Zustand der Ladung des Fahrzeugs 1" zu überwachen und gegebenenfalls zu
25 beeinflussen. Handelt es sich beispielsweise bei dem Container 15 um einen Kühlcontainer und wird über die Erfassungseinrichtung ein Anstieg der Temperatur im Container 15 über einen vorgegebenen Grenzwert ermittelt, so kann in der oben beschriebenen Weise über die Datenzentrale eine Betriebsbeeinflussung erfolgen. Hierzu kann beispielsweise durch entsprechende von der Datenzentrale übermittelte Betriebsbeeinflussungsdaten die Kühlleistung des Kühlaggregats 15.2 des Containers 15 erhöht werden. Zudem kann durch die
30 gespeicherten und in der oben beschriebenen Weise authentifizierten Protokolldatensätze gegebenenfalls zweifelsfrei der Temperaturverlauf im Inneren des Containers 15 nachgewiesen werden. Dies kann beispielsweise beim Transport von verderblichen Lebensmitteln,

wie Fleisch oder dergleichen, dazu verwendet werden, nachzuweisen, dass die Temperatur der Lebensmittel für die Zeit, die sie im Inneren des Containers 15 aufbewahrt wurden, stets unterhalb vorgeschriebener Grenzwerte lag.

Weiterhin ist es durch die Ermittlung der Position des Fahrzeugs 1" durch die Erfassungseinrichtung 14 insbesondere möglich, den Standort der Container 15 und 16 nachzuvollziehen. Insbesondere können diese Erkenntnisse in eine übergeordnete Logistikplanung einfließen.

Die Positionsbestimmung durch die Erfassungseinrichtung 14 kann in beliebiger bekannter Weise erfolgen. So kann die Erfassungseinrichtung 14 ein entsprechendes GPS-Modul.

Ebenso kann aber auch in bekannter Weise eine Positionsbestimmung über das Mobilfunknetz 3" erfolgen.

Auch hier sei erwähnt, dass die Kommunikation zwischen dem Fahrzeug 1" und der Datenzentrale wie die oben im Zusammenhang mit Figur 1 beschriebene Kommunikation abläuft. Insbesondere findet jeweils eine starke wechselseitige Authentifizierung unter Verwendung kryptographischer Mittel statt, sodass in Verbindung mit der Authentifizierung der ersten Daten jeweils gewährleistet ist, dass nur autorisierte und authentische Daten ausgetauscht und verwendet werden.

Die vorliegende Erfindung wurde vorstehend ausschließlich anhand von Beispielen für Fahrzeuge beschrieben. Es versteht sich jedoch, dass Erfindung auch im Zusammenhang mit beliebigen anderen beweglichen Einrichtungen, wie beispielsweise Containern etc. zur Anwendung kommen kann.

* * * * *

Patentansprüche

1. Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1''), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') erfolgt, dadurch gekennzeichnet, dass die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.
5
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung einer ersten Quelle (1.2, 4, 5; 8) der ersten Daten eine erste Quellenidentifikation umfassen.
10
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung eines ersten Empfängers (2.2) der ersten Daten eine erste Empfängeridentifikation umfassen.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten zur Authentifizierung der Übertragung der ersten Daten eine Übertragungsidentifikation umfassen.
15
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten wenigstens eine für ein vorgegbares Ereignis charakteristische Zeitkennung umfassen.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die authentifizierten ersten Daten in einen Protokolldatensatz eingefügt werden, der in der ersten Einrichtung (1; 1'; 1'') und/oder der Datenzentrale (2; 2') gespeichert wird.
20
7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten unter Verwendung wenigstens einer ersten digitalen Signatur authentifiziert werden.
25
8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Er-

fassungswert einer ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) der ersten Einrichtung (1; 1'; 1'') erfasst wurde.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass die erste Erfassungsgröße eine Zustandsgröße der ersten Einrichtung (1; 1'; 1'') ist.
10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Daten wenigstens Betriebsbeeinflussungsdaten umfassen, die zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'') an die erste Einrichtung (1; 1'; 1'') übermittelt werden.
11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Daten über wenigstens eine zweite Datenübertragungseinrichtung (3.1; 8.2) übertragen werden.
12. Verfahren zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, bei dem zwischen der mobilen ersten Einrichtung (1; 1'; 1'') und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2') über wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') erste Daten mit einem Verfahren nach einem der vorhergehenden Ansprüche übertragen werden, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, wobei
 - die ersten Überwachungsdaten wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, der von einer ersten Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) der ersten Einrichtung erfasst wurde,
 - die ersten Überwachungsdaten in der Datenzentrale (2; 2') verifiziert werden und
 - die ersten Überwachungsdaten bei erfolgreicher Verifikation in der Datenzentrale (2; 2') analysiert werden.
13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass in der Datenzentrale (2; 2') in Abhängigkeit von der Analyse der ersten Überwachungsdaten eine erste Überwachungsreaktion ausgelöst wird.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die erste Überwachungsreaktion einen Abrechnungsvorgang umfasst.
15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die erste Überwachungsreaktion die Generierung von Betriebsbeeinflussungsdaten umfasst, die zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'') an die erste Einrichtung (1; 1'; 1'') übermittelt werden.
16. Verfahren nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, dass bei der Analyse weitere, nicht von der ersten Einrichtung (1; 1'; 1'') übermittelte Daten berücksichtigt werden.
17. Anordnung zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung, insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei zur Übertragung der Daten wenigstens eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') vorgesehen ist, dadurch gekennzeichnet, dass die übertragenen Daten erste Daten umfassen und wenigstens eine Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') vorgesehen ist, die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.
18. Anordnung nach Anspruch 17, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zur Authentifizierung einer ersten Quelle (1.2, 4, 5; 8) der ersten Daten zum Einbringen einer ersten Quellenidentifikation in den ersten Datensatz ausgebildet ist.
19. Anordnung nach Anspruch 17 oder 18, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zur Authentifizierung eines ersten Empfängers (2.2) der ersten Daten zum Einbringen einer ersten Empfängeridentifikation in den ersten Datensatz ausgebildet ist.
20. Anordnung nach einem der Ansprüche 17 bis 19, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2; 1.2'; 1.2'') zur Authentifizierung der Übertragung der ersten Daten zum Einbringen einer Übertragungsidentifikation in den ersten Datensatz ausgebildet ist.
21. Anordnung nach einem der Ansprüche 17 bis 20, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zum Einbringen wenigstens einer für ein

vorgebbares Ereignis charakteristischen Zeitkennung in den ersten Datensatz ausgebildet ist.

22. Anordnung nach einem der Ansprüche 17 bis 21, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zum Einbringen der authentifizierten ersten Daten in einen Protokolldatensatz ausgebildet ist und dass die erste Einrichtung (1; 1'; 1'') einen ersten Protokollspeicher (1.5) zum Speichern des Protokolldatensatzes aufweist und/oder die Datenzentrale (2; 2') einen zweiten Protokollspeicher (2.3) zum Speichern des Protokolldatensatzes aufweist.
23. Anordnung nach einem der Ansprüche 17 bis 22, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (1.2, 2.2; 1.2'; 1.2'') zur Bildung einer ersten digitalen Signatur unter Verwendung der ersten Daten ausgebildet ist.
24. Anordnung nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass die erste Einrichtung (1; 1'; 1'') eine erste Sicherheitseinrichtung (1.2; 1.2'; 1.2'') umfasst und/oder die Datenzentrale (2; 2') eine zweite Sicherheitseinrichtung (2.2) umfasst.
25. Anordnung nach einem der Ansprüche 17 bis 24, dadurch gekennzeichnet, dass die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale (2; 2') übertragene erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, wobei die erste Einrichtung eine erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung des ersten Erfassungswerts umfasst.
26. Anordnung nach Anspruch 25, dadurch gekennzeichnet, dass die erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung einer Zustandsgröße der ersten Einrichtung (1; 1'; 1'') als erster Erfassungsgröße ausgebildet ist.
27. Anordnung nach einem der Ansprüche 17 bis 26, dadurch gekennzeichnet, dass die ersten Daten von der Datenzentrale (2; 2') zur ersten Einrichtung (1; 1'; 1'') übertragene Betriebsbeeinflussungsdaten umfassen, wobei die erste Einrichtung (1; 1'; 1'') eine Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'', 15) in Abhängigkeit von den Betriebsbeeinflussungsdaten aufweist.

28. Anordnung nach einem der Ansprüche 17 bis 27, dadurch gekennzeichnet, dass zur Datenübertragung zwischen der ersten Einrichtung (1; 1') und der Datenzentrale (2; 2') wenigstens eine zweite Datenübertragungseinrichtung (3.1; 8.2) vorgesehen ist.

29. Anordnung zur Überwachung einer mobilen ersten Einrichtung, insbesondere eines Fahrzeugs, mit einer Anordnung zur Übertragung von ersten Daten nach einem der Ansprüche 17 bis 28, dadurch gekennzeichnet, dass

- die ersten Daten von der ersten Einrichtung (1; 1'; 1'') zur Datenzentrale übertragene (2; 2') erste Überwachungsdaten umfassen, die wenigstens einen ersten Erfassungswert einer ersten Erfassungsgröße umfassen, wobei die erste Einrichtung (1; 1'; 1'') eine erste Erfassungseinrichtung (4, 5; 10; 14, 15.1, 16.1) zur Erfassung des ersten Erfassungswerts umfasst,
- die Datenzentrale (2; 2') eine zweite Sicherheitseinrichtung (2.2) zum Verifizieren der ersten Überwachungsdaten aufweist und
- die Datenzentrale (2; 2') eine mit der zweiten Sicherheitseinrichtung (2.2) verbundene Analyseeinrichtung (2.4) zum Analysieren der ersten Überwachungsdaten in Abhängigkeit vom Ergebnis der Verifikation aufweist.

30. Anordnung nach Anspruch 29, dadurch gekennzeichnet, dass wenigstens eine mit der Analyseeinrichtung (2.4) verbindbare Überwachungsreaktionseinrichtung (2.5, 2.6, 2.7) zur Durchführung einer ersten Überwachungsreaktion vorgesehen ist und die Analyseeinrichtung (2.4) zum Ansteuern der Überwachungsreaktionseinrichtung (2.5, 2.6, 2.7) zum Auslösen einer ersten Überwachungsreaktion in Abhängigkeit vom Ergebnis der Analyse der ersten Überwachungsdaten ausgebildet ist.

31. Anordnung nach Anspruch 30, dadurch gekennzeichnet, dass als Überwachungsreaktionseinrichtung eine mit der Analyseeinrichtung (2.4) verbindbare Abrechnungseinrichtung (2.5) vorgesehen ist.

32. Anordnung nach Anspruch 30 oder 31, dadurch gekennzeichnet, dass

- die Überwachungsreaktionseinrichtung (2.6, 2.7) zur Generierung von Betriebsbeeinflussungsdaten zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'', 15) als erste Überwachungsreaktion ausgebildet ist,

- die Datenzentrale (2; 2') zur Übertragung erster Daten an die erste Einrichtung (1; 1'; 1'') ausgebildet ist, wobei die ersten Daten die Betriebsbeeinflussungsdaten umfassen, und
- die erste Einrichtung (1; 1'; 1'') eine Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung in Abhängigkeit von den Betriebsbeeinflussungsdaten aufweist.

33. Anordnung nach Anspruch 32, dadurch gekennzeichnet, dass

- die erste Einrichtung (1; 1'; 1'') eine erste Sicherheitseinrichtung (1.2; 1.2'; 1.2'') umfasst, die zum Verifizieren der die Betriebsbeeinflussungsdaten umfassenden ersten Daten ausgebildet ist und
- die Betriebsbeeinflussungseinrichtung (6; 10; 15.1) zur Beeinflussung des Betriebs der ersten Einrichtung (1; 1'; 1'', 15) in Abhängigkeit vom Ergebnis der Verifizierung ausgebildet ist.

34. Anordnung nach einem der Ansprüche 29 bis 33, dadurch gekennzeichnet, dass die Analyseeinrichtung (2.4) zur Berücksichtigung weiterer, nicht von der ersten Einrichtung übermittelter Daten ausgebildet ist.

35. Mobile erste Einrichtung, insbesondere Fahrzeug, für eine Anordnung nach einem der Ansprüche 17 bis 34, gekennzeichnet durch eine erste Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') zur Übertragung erster Daten und eine mit der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') verbindbare erste Sicherheitseinrichtung (1.2; 1.2'; 1.2''), die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

36. Mobile erste Einrichtung nach Anspruch 35, dadurch gekennzeichnet, dass die erste Sicherheitseinrichtung (1.2; 1.2'; 1.2'') zur Authentifizierung der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') zum Einbringen einer der ersten Datenübertragungseinrichtung (1.1; 1.1'; 1.1'') zugeordneten Identifikation in den ersten Datensatz ausgebildet ist.

37. Datenzentrale für eine Anordnung nach einem der Ansprüche 17 bis 34, gekennzeichnet durch eine Datenübertragungseinrichtung (2.1) zur Übertragung erster Da-

ten und eine mit der Datenübertragungseinrichtung (2.1) verbindbare zweite Sicherheitseinrichtung (2.2), die zum Generieren eines die ersten Daten darstellenden ersten Datensatzes und zum Authentifizieren der ersten Daten durch kryptographische Mittel ausgebildet ist.

5

* * * * *

Zusammenfassung

Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung (1; 1'; 1''), insbesondere einem Fahrzeug, und einer von der ersten Einrichtung (1; 1'; 1'') zumindest zeitweise entfernten Datenzentrale (2; 2'), wobei die Übertragung der Daten über wenigstens
5 eine mobile erste Übertragungseinrichtung (1.1; 1.1'; 1.1'') erfolgt und die übertragenen Daten erste Daten umfassen, die durch kryptographische Mittel authentifiziert werden.

Figur 1

* * * * *

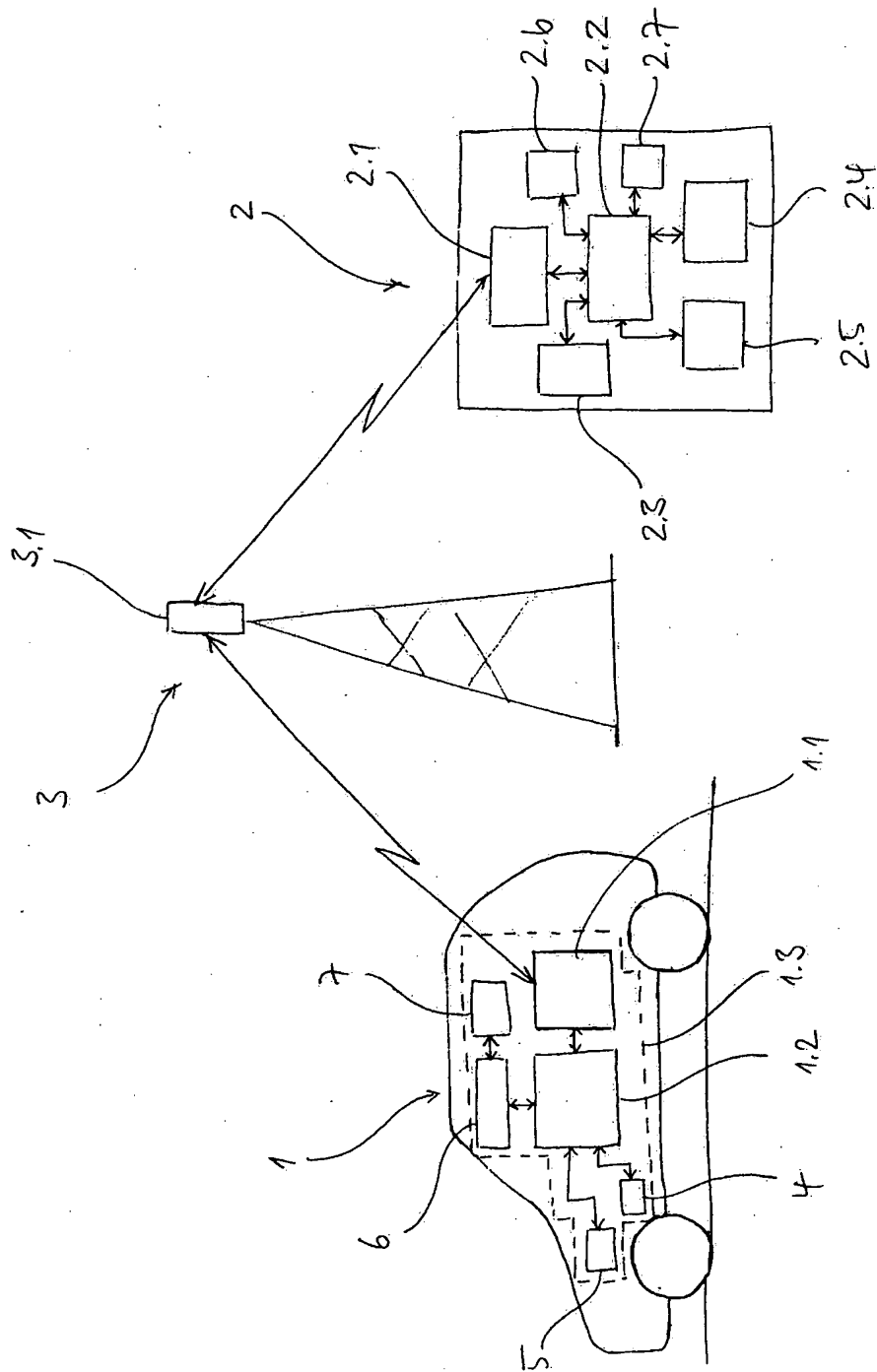


Fig. 1

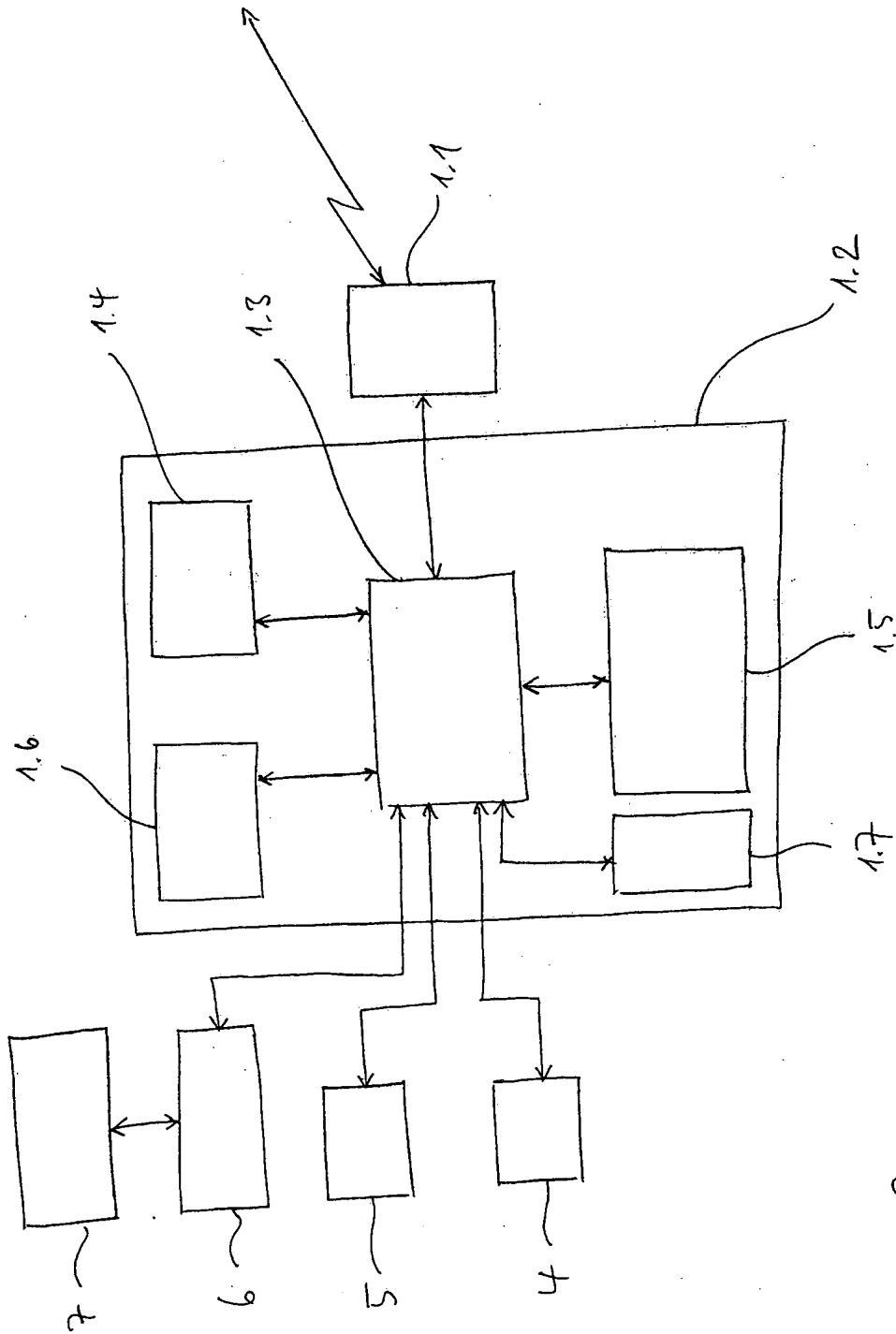


Fig. 2

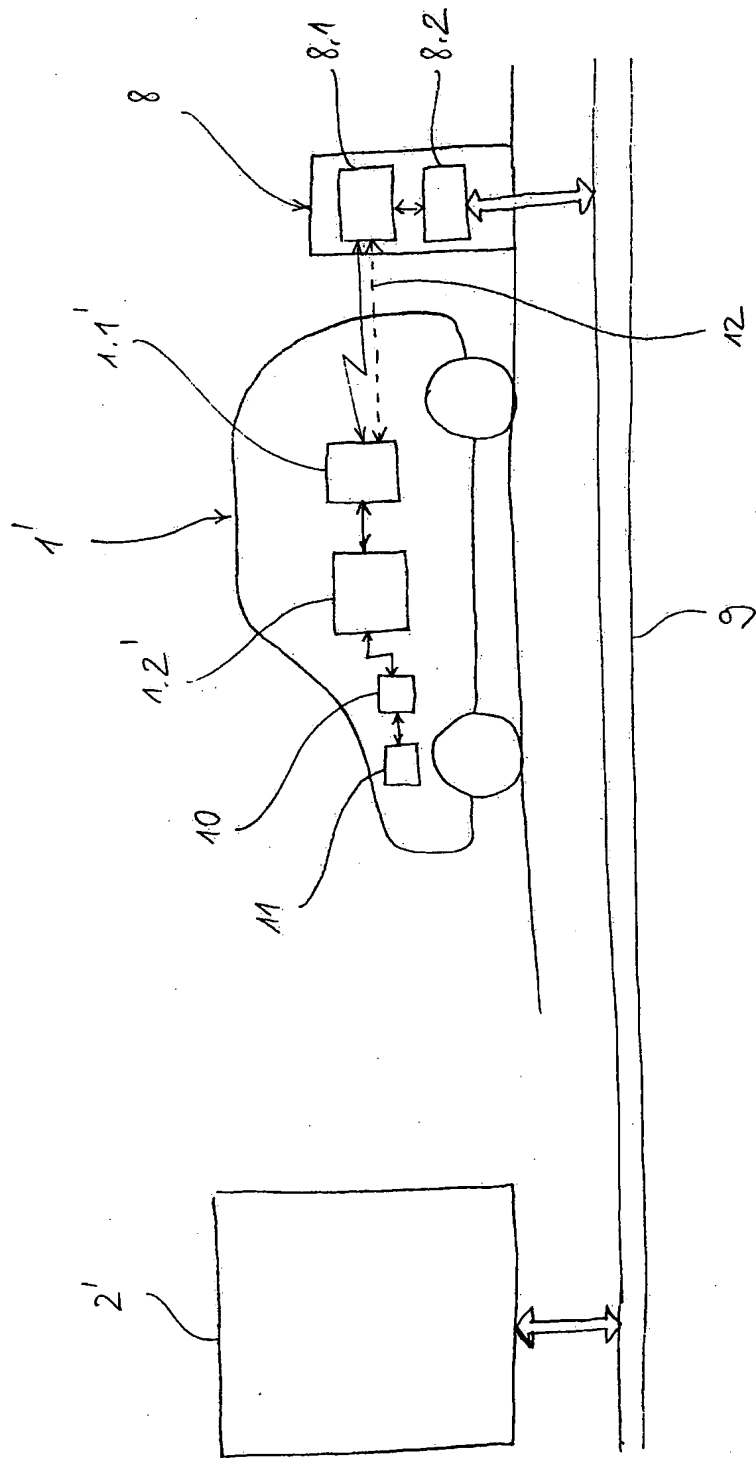


Fig. 3

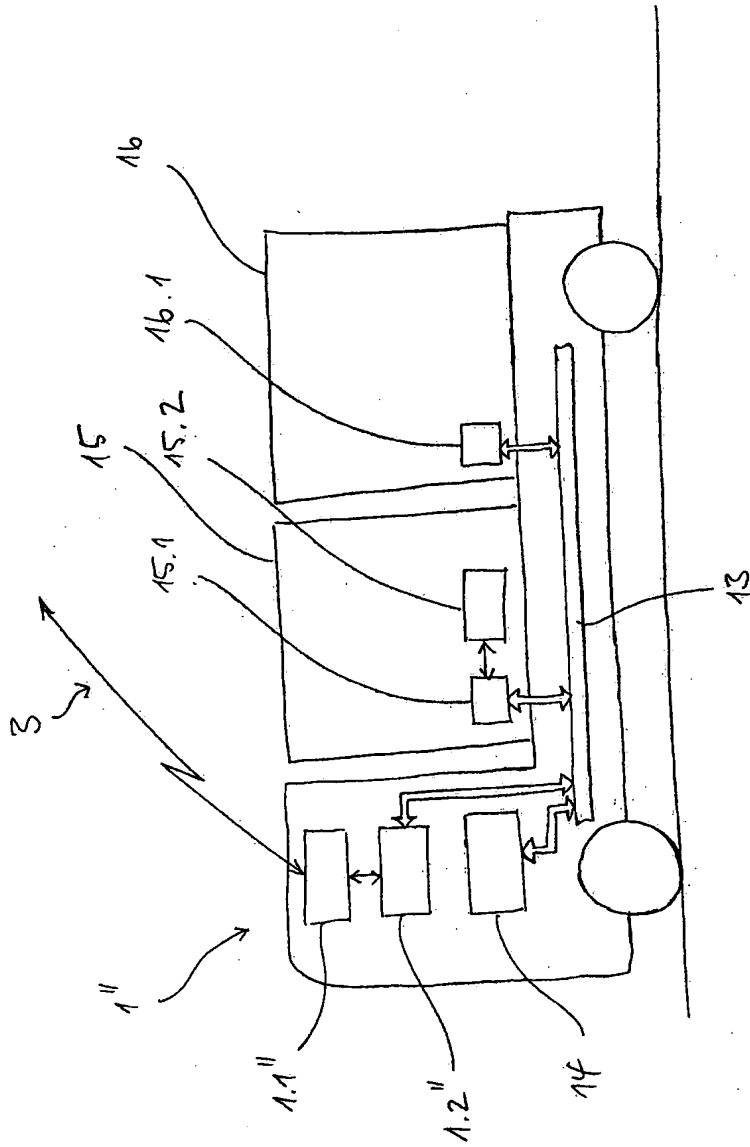


Fig. 4

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Rec'd PCT/PTO 21 JUL 2005

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

REC'D 15 JUN 2004

PCT WIPO PC

An:

siehe Formular PCT/ISA/220

SCHRIFTLICHER BESCHIED DER INTERNATIONALEN RECHERCHENBEHÖRDE (Regel 43bis.1 PCT)

Absendedatum

(Tag/Monat/Jahr) siehe Formular PCT/ISA/210 (Blatt 2)

Aktenzeichen des Anmelders oder Anwalts
siehe Formular PCT/ISA/220

WEITERES VORGEHEN siehe Punkt 2 unten

Internationales Aktenzeichen
PCT/EP2004/000505

Internationales Anmeldedatum (Tag/Monat/Jahr)
22.01.2004

Prioritätsdatum (Tag/Monat/Jahr)
22.01.2003

Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK
G07B15/00, B60R16/00, H04L29/06

Anmelder
FRANCOTYP-POSTALIA AG & CO. KG

1. Dieser Bescheid enthält Angaben zu folgenden Punkten:

- ☒ Feld Nr. I Grundlage des Bescheids
- ☒ Feld Nr. II Priorität
- ☐ Feld Nr. III Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- ☐ Feld Nr. IV Mangelnde Einheitlichkeit der Erfindung
- ☒ Feld Nr. V Begründete Feststellung nach Regel 43bis.1(a)(i) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- ☐ Feld Nr. VI Bestimmte angeführte Unterlagen
- ☒ Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung
- ☒ Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung

2. WEITERES VORGEHEN

Wird ein Antrag auf internationale vorläufige Prüfung gestellt, so gilt dieser Bescheid als schriftlicher Bescheid der mit der internationalen vorläufigen Prüfung beauftragten Behörde ("IPEA"); dies trifft nicht zu, wenn der Anmelder eine andere Behörde als diese als IPEA wählt und die gewählte IPEA dem Internationale Büro nach Regel 66.1bis b) mitgeteilt hat, daß schriftliche Bescheide dieser Internationalen Recherchenbehörde nicht anerkannt werden.

Wenn dieser Bescheid wie oben vorgesehen als schriftlicher Bescheid der IPEA gilt, so wird der Anmelder aufgefordert, bei der IPEA vor Ablauf von 3 Monaten ab dem Tag, an dem das Formblatt PCT/ISA/220 abgesandt wurde oder vor Ablauf von 22 Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft, eine schriftliche Stellungnahme und, wo dies angebracht ist, Änderungen einzureichen.

Weitere Optionen siehe Formblatt PCT/ISA/220.

3. Nähere Einzelheiten siehe die Anmerkungen zu Formblatt PCT/ISA/220.

Name und Postanschrift der mit der internationalen Recherchenbehörde



Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Kopp, K

Tel. +49 89 2399-7833



Feld Nr. I Grundlage des Bescheids

1. Hinsichtlich der **Sprache** ist der Bescheid auf der Grundlage der internationalen Anmeldung in der Sprache erstellt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
 - ☐ Der Bescheid ist auf der Grundlage einer Übersetzung aus der Originalsprache in die folgende Sprache erstellt worden, bei der es sich um die Sprache der Übersetzung handelt, die für die Zwecke der internationalen Recherche eingereicht worden ist (gemäß Regeln 12.3 und 23.1 b)).
2. Hinsichtlich der **Nucleotid- und/oder Aminosäuresequenz**, die in der internationalen Anmeldung offenbart wurde und für die beanspruchte Erfindung erforderlich ist, ist der Bescheid auf folgender Grundlage erstellt worden:
 - a. Art des Materials
 - ☐ Sequenzprotokoll
 - ☐ Tabelle(n) zum Sequenzprotokoll
 - b. Form des Materials
 - ☐ in schriftlicher Form
 - ☐ in computerlesbarer Form
 - c. Zeitpunkt der Einreichung
 - ☐ in der eingereichten internationalen Anmeldung enthalten
 - ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht
 - ☐ bei der Behörde nachträglich für die Zwecke der Recherche eingereicht
3. ☐ Wurden mehr als eine Version oder Kopie eines Sequenzprotokolls und/oder einer dazugehörigen Tabelle eingereicht, so sind zusätzlich die erforderlichen Erklärungen, daß die Information in den nachgereichten oder zusätzlichen Kopien mit der Information in der Anmeldung in der eingereichten Fassung übereinstimmt bzw. nicht über sie hinausgeht, vorgelegt worden.
4. Zusätzliche Bemerkungen:

Feld Nr. II Priorität

1. ☒ Das folgende Dokument ist noch nicht eingereicht worden:
- ☒ Abschrift der früheren Anmeldung, deren Priorität beansprucht worden ist (Regel 43*bis*.1 und 66.7(a)).
 - ☐ Übersetzung der früheren Anmeldung, deren Priorität beansprucht worden ist (Regel 43*bis*.1 und 66.7(b)).

Daher war es nicht möglich, die Gültigkeit des Prioritätsanspruchs zu prüfen. Der Bescheid wurde trotzdem in der Annahme erstellt, daß das beanspruchte Prioritätsdatum das maßgebliche Datum ist.

2. ☐ Dieser Bescheid ist ohne Berücksichtigung der beanspruchten Priorität erstellt worden, da sich der Prioritätsanspruch als ungültig erwiesen hat (Regeln 43*bis*.1 und 64.1). Für die Zwecke dieses Bescheids gilt daher das vorstehend genannte internationale Anmeldedatum als das maßgebliche Datum.

3. Etwaige zusätzliche Bemerkungen:

Feld Nr. V Begründete Feststellung nach Regel 43*bis*.1(a)(i) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit	Ja: Ansprüche 10,24,27,29-34 Nein: Ansprüche 1-9,11-23,25-26,28,35-37
Erfinderische Tätigkeit	Ja: Ansprüche Nein: Ansprüche 1-37
Gewerbliche Anwendbarkeit	Ja: Ansprüche: 1-37 Nein: Ansprüche:

2. Unterlagen und Erklärungen:

siehe Beiblatt

Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

Zu Punkt I

Grundlage des Bescheides

Der Prüfung werden **folgende Anmeldungsunterlagen** zugrunde gelegt:

Beschreibung, Seiten:

1-30

ursprüngliche Fassung

Patentansprüche, Nr.:

1-37

ursprüngliche Fassung

Zeichnungen, Blätter:

1/4-4/4

ursprüngliche Fassung

Zu Punkt V

Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Es wird auf folgende Dokumente verwiesen:

D1: WO 01/59711

D2: US 2002/0034301

D3: EP 0780801

D4: WO 02/15149

2. Der Anspruch 1 ist nicht neu (Artikel 33(2) PCT).

Das Dokument D1 wird als nächstliegender Stand der Technik angesehen und offenbart die folgenden Merkmale des Anspruches (die Verweise beziehen sich auf dieses Dokument) soweit Anspruch 1 klar ist:

- Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung und einer von der ersten Einrichtung zumindest zweitweise entfernten Datenzentrale, wobei die Übertragung der Daten über wenigstens eine mobile erste Datenübertragungseinrichtung erfolgt (Seite 3, Zeilen 25-27),
dadurch gekennzeichnet,
 - dass die übertragenen Daten erste Daten umfassen, die durch kryptografische Mittel authentifiziert werden (Seite 3, Zeilen 27-28).
- 3. Die Merkmale des Anspruchs 1 sind ebenso in Dokument D2 (z.B. Absatz 3, Absatz 18) offenbart.
- 4. Der Anspruch 17 korrespondiert zu Anspruch 1, die Feststellungen zu Anspruch 1 gelten entsprechend. Deshalb ist Anspruch 17 nicht neu (Artikel 33(2) PCT).
- 5. Wenn, basierend auf geringfügigen Änderungen der Interpretation, Neuheit strittig wäre, wird darauf hingewiesen, daß der Gegenstand der unabhängigen Ansprüche 1 und 17 keine erfinderische Tätigkeit enthält (Artikel 33(3) PCT).
- 6. Die abhängigen Ansprüche enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf die sie sich rückbeziehen, die Erfordernisse des PCT in bezug auf Neuheit bzw. erfinderische Tätigkeit erfüllen. Die Merkmale sind entweder in D1 offenbart (z.B. "die authentifizierten ersten Daten werden in einen Protokolldatensatz eingefügt und in der ersten Einrichtung gespeichert"), D3 (z.B. "die erste Überwachungsreaktion umfasst einen Abrechnungsvorgang"), D4 (z.B. die ersten Überwachungsdaten umfassen eine ersten Erfassungswert einer ersten Erfassungsgröße"; "die ersten Überwachungsdaten werden in der Datenzentrale analysiert") oder offensichtlich für den Fachmann (z.B. "die Daten umfassen eine Zeitkennung").

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

1. Wenn neue unabhängige Ansprüche eingereicht werden, sind diese vis-à-vis D1 zu formulieren (Regel 6.3 (b) PCT).

2. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der in den Dokumenten D1-D2 offenbarte einschlägige Stand der Technik noch diese Dokumente angegeben.
3. Ein Teil des Gegenstandes der Beschreibung wird nicht von den Ansprüchen umfasst (Seite 14, Zeilen 25-34, Seite 30, Zeilen 8-11). Diese Inkonsistenz zwischen den Ansprüchen und der Beschreibung führt zu Zweifeln über den Schutzbereich und daher zur Unklarheit (Artikel 6 PCT).
4. Die verschwommene und unpräzise Angaben in der Beschreibung auf Seite 30, Zeilen 19-21 erwecken den Eindruck, daß der Gegenstand, für den Schutz begehrt wird, nicht dem in den Ansprüchen definierten Gegenstand entspricht, und führen daher zur Unklarheit (Artikel 6 PCT), wenn die Beschreibung zur Auslegung der Ansprüche herangezogen wird.
5. Der Anmelder wird gebeten, die Änderungen auf Austauschseiten wie in Regel 66.8 a) PCT vorgeschrieben einzureichen.

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

1. Die Ansprüche, die nicht den Erfordernissen des Artikel 6 PCT genügen:
 - 1.1 Der Ausdruck
 - "insbesondere", verwendet in den Ansprüchen 1, 12, 17, 29, 35; führt zu Zweifeln über den Schutzbereich (s.a. PCT Gazette, Sektion IV III-4.6), weil nicht klar ist, ob die diesem Ausdruck folgenden Merkmale zum beanspruchten Schutzbereich gehören oder nicht.
 - 1.2 Die Ausdrücke
 - "zumindest zeitweise entfernte Datenzentrale", verwendet in den Ansprüchen 1, 12, 17;
 - "ein vorgebbares Ereignis", verwendet in Anspruch 5, 21; haben keine allgemein anerkannte Bedeutung und führen daher zu Zweifeln über

den Schutzbereich der Gegenstände der jeweiligen Ansprüche.

1.3 Es ist unklar, ob mit den Begriffen

- "einer mobilen ersten Einrichtung" und "der ersten Einrichtung", verwendet in den Ansprüchen 1, 12, 17;
- "erste Daten", verwendet in Anspruch 1 und "die Daten", verwendet in Anspruch 11;

dieselbe Entität gemeint ist oder nicht.

1.4 In Anspruch 4 ist unklar, welches technische Merkmal mit dem Ausdruck "die ersten Daten zur Authentifizierung der Übertragung der ersten Daten umfassen eine Übertragungsidentifikation.

1.5 Der Ausdruck "weitere, nicht von der ersten Einrichtung übermittelte Daten", verwendet in den Ansprüchen 16 und 34 lässt den Leser im unklaren über die Bedeutung des technischen Merkmals auf das sich der Ausdruck bezieht und führt daher zu Zweifeln über den Schutzbereich.

1.6 Der Gegenstand der Ansprüche 10, 15, 27, 32, 33 ist durch das zu erreichende Ergebnis definiert und daher unklar.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

PCT

An
COHAUSZ & FLORACK
z.H. Karlhuber, Mathias
Bleichstrasse 14
D-40211 Düsseldorf
GERMANY

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES
INTERNATIONALEN RECHERCHENBERICHTS
UND DES SCHRIFTLICHEN BESCHEIDS DER
INTERNATIONALEN RECHERCHENBEHÖRDE
ODER DER ERKLÄRUNG

Eingang: 21. JUNI 2004

(Regel 44.1 PCT)

Absenddatum
(Tag/Monat/Jahr)

17/06/2004

Aktenzeichen des Anmelders oder Anwalts

KA/nw 030992WO

WEITERES VORGEHEN

siehe Punkte 1 und 4 unten

Internationales Aktenzeichen

PCT/EP2004/000505

Internationales Anmeldedatum

(Tag/Monat/Jahr)

22/01/2004

Anmelder

FRANCOTYP-POSTALIA AG & CO. KG

1. ☒ Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht und der schriftliche Bescheid der Internationalen Recherchenbehörde erstellt wurden und ihm hiermit übermittelt werden.
Einreichung von Änderungen und einer Erklärung nach Artikel 19:
Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):
Bis wann sind Änderungen einzureichen?
Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts.
Wo sind Änderungen einzureichen?
Unmittelbar beim Internationalen Büro der WIPO, 34, chemin des Colombettes, CH-1211 Genf 20, Telefaxnr.: (41-22) 740.14.35
Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.
2. ☐ Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17 (2) a) sowie der schriftliche Bescheid der Internationalen Recherchenbehörde übermittelt werden.
3. ☐ **Hinsichtlich des Widerspruchs** gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß
☐ der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.
☐ noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.
4. **Zur Erinnerung:**
Kurz nach Ablauf von **18 Monaten** seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90^{bis}.1 bzw. 90^{bis}.3 vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.
Der Anmelder kann beim Internationalen Büro eine informelle Stellungnahme zum schriftlichen Bescheid der Internationalen Recherchenbehörde einreichen. Das Internationale Büro sendet allen Bestimmungsämtern eine Kopie dieser Stellungnahme, sofern nicht ein internationaler vorläufiger Prüfungsbericht erstellt worden ist bzw. gerade erstellt wird. Eine solche Stellungnahme würde auch der Öffentlichkeit zugänglich gemacht, allerdings erst nach Ablauf von 30 Monaten seit dem Prioritätsdatum.
In bezug auf einige Bestimmungsämter ist innerhalb von **19 Monaten** seit dem Prioritätsdatum ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase verschieben und erst **30 Monaten** nach dem Prioritätsdatum (in manchen Ämtern sogar noch später) vornehmen möchte; ansonsten muß der Anmelder innerhalb von **20 Monaten** seit dem Prioritätsdatum die für den Eintritt in die nationale Phase vor diesen Bestimmungsämtern vorgeschriebenen Handlungen vornehmen.
Bei anderen Bestimmungsämtern gilt die Frist von **30 Monaten** (oder eine etwaige längere Frist) auch dann, wenn innerhalb von 19 Monaten kein solcher Antrag eingereicht wird.
Siehe Anhang zu Formblatt PCT/IB/301. Genaue Angaben zu den jeweils geltenden Fristen in den einzelnen Ämtern enthält der **PCT-Leitfaden für Anmelder**, Band II, Nationale Kapitel sowie die Website der WIPO.

Name und Postanschrift der Internationalen Recherchenbehörde



Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Ainhua Barrio Baranano

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.

Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Ansprüche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen die anderen Ansprüche nicht neu numeriert zu werden. Im Fall einer Neunumerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

- i) der Anspruch unverändert ist;
- ii) der Anspruch gestrichen worden ist;
- iii) der Anspruch neu ist;
- iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;
- v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."
2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."
3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:
"Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt. "Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."
4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigefügt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amtes sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

PATENT COOPERATION TREATY

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts KA/nw 030992WO	WEITERES VORGEHEN	siehe Formblatt PCT/ISA/220 sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/EP2004/000505	Internationales Anmeldedatum (Tag/Monat/Jahr) 22/01/2004	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 22/01/2003
Anmelder FRANCOTYP-POSTALIA AG & CO. KG		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 4 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. ☐ Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** siehe Feld Nr. 1.

2. ☐ **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld II).

3. ☐ **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld III).

4. Hinsichtlich der Bezeichnung der Erfindung

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld Nr. IV angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Hinsichtlich der Zeichnungen

- a. ist folgende Abbildung der **Zeichnungen** mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☒ wie vom Anmelder vorgeschlagen

☐ wie von der Behörde ausgewählt, weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ wie von der Behörde ausgewählt, weil diese Abbildung die Erfindung besser kennzeichnet.

- b. ☐ wird keine der Abbildungen mit der Zusammenfassung veröffentlicht.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 IPK 7 G07B15/00 B60R16/00 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G07B B60R H04L G06F G07F G08G B61L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, COMPENDEX

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y	<p>WO 01/59711 A (RIEDER HELMUT ;EFKON AG (AT); PAMMER RAIMUND (AT)) 16. August 2001 (2001-08-16)</p> <p>Zusammenfassung Seite 1, Absatz 1 Seite 3, letzter Absatz -Seite 4, Absatz 1 Seite 6, Absatz 3 -Seite 8, Absatz 1 Abbildungen 1,2</p> <p style="text-align: center;">--- -/-</p>	<p>1-9, 11-23, 25, 26, 28, 35-37 10, 24, 27, 29-34</p>

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

G Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

4. Juni 2004

Absendedatum des internationalen Recherchenberichts

17/06/2004

Name und Postanschrift der Internationalen Recherchenbehörde
 Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Kopp, K

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	<p>US 2002/034301 A1 (ANDERSSON STEFAN) 21. März 2002 (2002-03-21) Absatz '0003! - Absatz '0004! Absatz '0006! - Absatz '0007! Absatz '0018! - Absatz '0022! Absatz '0029! - Absatz '0030! Abbildung 3 Ansprüche 1,8</p> <p style="text-align: center;">----</p>	<p>1-4,6, 17-20,23</p>
Y	<p>EP 0 780 801 A (GZS GES FUER ZAHLUNGSSYSTEME M) 25. Juni 1997 (1997-06-25) Seite 12, Zeile 46 - Zeile 54 Seite 13, Zeile 35 - Zeile 38 Seite 15, Zeile 26 -Seite 16, Zeile 31 Seite 26, Zeile 28 -Seite 27, Zeile 53 Seite 35, Zeile 21 -Seite 36, Zeile 3 Seite 36, Zeile 35 -Seite 37, Zeile 13 Seite 38, Zeile 8 - Zeile 16 Seite 39, Zeile 6 - Zeile 13</p> <p style="text-align: center;">---</p>	<p>10,24, 27,29-34</p>
A	<p>WO 02/15149 A (NEW FLYER IND ;PACHET EUGENE (CA); HARVEY LEE (CA)) 21. Februar 2002 (2002-02-21) Zusammenfassung Seite 1, Zeile 9 - Zeile 18 Seite 2, Zeile 7 - Zeile 8 Seite 2, Zeile 16 -Seite 3, Zeile 22 Seite 5, Zeile 20 - Zeile 25 Seite 7, Zeile 22 -Seite 10, Zeile 19 Seite 21, Zeile 7 - Zeile 11 Abbildung 3A</p> <p style="text-align: center;">-----</p>	<p>1-37</p>

INTERNATIONALE RESEARCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2004/000505

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0159711 A	16-08-2001	WO 0159711 A1	16-08-2001
		AT 1992000 A	15-01-2004
		AT 246384 T	15-08-2003
		AU 3347201 A	20-08-2001
		DE 50100441 D1	04-09-2003
		EP 1254434 A1	06-11-2002
		ES 2203590 T3	16-04-2004
		JP 2003526854 T	09-09-2003
		NO 20023718 A	06-08-2002
		PT 1254434 T	31-12-2003
		US 2003011494 A1	16-01-2003
		ZA 200205601 A	14-07-2003
US 2002034301 A1	21-03-2002	GB 2366139 A	27-02-2002
		AU 8394901 A	25-02-2002
		WO 0215626 A1	21-02-2002
		EP 1323323 A1	02-07-2003
EP 0780801 A	25-06-1997	AU 1432697 A	14-07-1997
		WO 9722953 A1	26-06-1997
		EP 0780801 A1	25-06-1997
WO 0215149 A	21-02-2002	AU 5808801 A	25-02-2002
		AU 6195001 A	25-02-2002
		AU 6195101 A	25-02-2002
		WO 0215149 A1	21-02-2002
		WO 0215150 A1	21-02-2002
		WO 0215151 A1	21-02-2002
		US 6556899 B1	29-04-2003
		US 6611739 B1	26-08-2003
		US 6681174 B1	20-01-2004

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

An:

siehe Formular PCT/ISA/220

PCT

SCHRIFTLICHER BESCHEID DER INTERNATIONALEN RECHERCHENBEHÖRDE (Regel 43bis.1 PCT)

Absendedatum

(Tag/Monat/Jahr) siehe Formular PCT/ISA/210 (Blatt 2)

Aktenzeichen des Anmelders oder Anwalts
siehe Formular PCT/ISA/220

WEITERES VORGEHEN
siehe Punkt 2 unten

Internationales Aktenzeichen
PCT/EP2004/000505

Internationales Anmeldedatum (Tag/Monat/Jahr)
22.01.2004

Prioritätsdatum (Tag/Monat/Jahr)
22.01.2003

Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK
G07B15/00, B60R16/00, H04L29/06

Anmelder
FRANCOTYP-POSTALIA AG & CO. KG

1. Dieser Bescheid enthält Angaben zu folgenden Punkten:

- ☒ Feld Nr. I Grundlage des Bescheids
- ☒ Feld Nr. II Priorität
- ☐ Feld Nr. III Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- ☐ Feld Nr. IV Mangelnde Einheitlichkeit der Erfindung
- ☒ Feld Nr. V Begründete Feststellung nach Regel 43bis.1(a)(i) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- ☐ Feld Nr. VI Bestimmte angeführte Unterlagen
- ☒ Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung
- ☒ Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung

2. WEITERES VORGEHEN

Wird ein Antrag auf internationale vorläufige Prüfung gestellt, so gilt dieser Bescheid als schriftlicher Bescheid der mit der internationalen vorläufigen Prüfung beauftragten Behörde ("IPEA"); dies trifft nicht zu, wenn der Anmelder eine andere Behörde als diese als IPEA wählt und die gewählte IPEA dem Internationale Büro nach Regel 66.1bis b) mitgeteilt hat, daß schriftliche Bescheide dieser Internationalen Recherchenbehörde nicht anerkannt werden.

Wenn dieser Bescheid wie oben vorgesehen als schriftlicher Bescheid der IPEA gilt, so wird der Anmelder aufgefordert, bei der IPEA vor Ablauf von 3 Monaten ab dem Tag, an dem das Formblatt PCT/ISA/220 abgesandt wurde oder vor Ablauf von 22 Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft, eine schriftliche Stellungnahme und, wo dies angebracht ist, Änderungen einzureichen.

Weitere Optionen siehe Formblatt PCT/ISA/220.

3. Nähere Einzelheiten siehe die Anmerkungen zu Formblatt PCT/ISA/220.

Name und Postanschrift der mit der internationalen
Recherchenbehörde



Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Kopp, K

Tel. +49 89 2399-7833



Feld Nr. I Grundlage des Bescheids

1. Hinsichtlich der **Sprache** ist der Bescheid auf der Grundlage der internationalen Anmeldung in der Sprache erstellt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
 - ☐ Der Bescheid ist auf der Grundlage einer Übersetzung aus der Originalsprache in die folgende Sprache erstellt worden, bei der es sich um die Sprache der Übersetzung handelt, die für die Zwecke der internationalen Recherche eingereicht worden ist (gemäß Regeln 12.3 und 23.1 b)).
2. Hinsichtlich der **Nucleotid- und/oder Aminosäuresequenz**, die in der internationalen Anmeldung offenbart wurde und für die beanspruchte Erfindung erforderlich ist, ist der Bescheid auf folgender Grundlage erstellt worden:
 - a. Art des Materials
 - ☐ Sequenzprotokoll
 - ☐ Tabelle(n) zum Sequenzprotokoll
 - b. Form des Materials
 - ☐ in schriftlicher Form
 - ☐ in computerlesbarer Form
 - c. Zeitpunkt der Einreichung
 - ☐ in der eingereichten internationalen Anmeldung enthalten
 - ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht
 - ☐ bei der Behörde nachträglich für die Zwecke der Recherche eingereicht
3. ☐ Wurden mehr als eine Version oder Kopie eines Sequenzprotokolls und/oder einer dazugehörigen Tabelle eingereicht, so sind zusätzlich die erforderlichen Erklärungen, daß die Information in den nachgereichten oder zusätzlichen Kopien mit der Information in der Anmeldung in der eingereichten Fassung übereinstimmt bzw. nicht über sie hinausgeht, vorgelegt worden.
4. Zusätzliche Bemerkungen:

**SCHRIFTLICHER BESCHEID DER
INTERNATIONALEN RECHERCHEBEHÖRDE**

Internationales Aktenzeichen
PCT/EP2004/000505

Feld Nr. II Priorität

1. ☒ Das folgende Dokument ist noch nicht eingereicht worden:

- ☒ Abschrift der früheren Anmeldung, deren Priorität beansprucht worden ist (Regel 43*bis*.1 und 66.7(a)).
- ☐ Übersetzung der früheren Anmeldung, deren Priorität beansprucht worden ist (Regel 43*bis*.1 und 66.7(b)).

Daher war es nicht möglich, die Gültigkeit des Prioritätsanspruchs zu prüfen. Der Bescheid wurde trotzdem in der Annahme erstellt, daß das beanspruchte Prioritätsdatum das maßgebliche Datum ist.

2. ☐ Dieser Bescheid ist ohne Berücksichtigung der beanspruchten Priorität erstellt worden, da sich der Prioritätsanspruch als ungültig erwiesen hat (Regeln 43*bis*.1 und 64.1). Für die Zwecke dieses Bescheids gilt daher das vorstehend genannte internationale Anmeldedatum als das maßgebliche Datum.

3. Etwaige zusätzliche Bemerkungen:

Feld Nr. V Begründete Feststellung nach Regel 43*bis*.1(a)(i) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit	Ja: Ansprüche 10,24,27,29-34 Nein: Ansprüche 1-9,11-23,25-26,28,35-37
Erfinderische Tätigkeit	Ja: Ansprüche Nein: Ansprüche 1-37
Gewerbliche Anwendbarkeit	Ja: Ansprüche: 1-37 Nein: Ansprüche:

2. Unterlagen und Erklärungen:

siehe Beiblatt

Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

Zu Punkt I

Grundlage des Bescheides

Der Prüfung werden **folgende Anmeldungsunterlagen** zugrunde gelegt:

Beschreibung, Seiten:

1-30

ursprüngliche Fassung

Patentansprüche, Nr.:

1-37

ursprüngliche Fassung

Zeichnungen, Blätter:

1/4-4/4

ursprüngliche Fassung

Zu Punkt V

**Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit
und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung
dieser Feststellung**

1. Es wird auf folgende Dokumente verwiesen:

D1: WO 01/59711

D2: US 2002/0034301

D3: EP 0780801

D4: WO 02/15149

2. Der Anspruch 1 ist nicht neu (Artikel 33(2) PCT).

Das Dokument D1 wird als nächstliegender Stand der Technik angesehen und offenbart die folgenden Merkmale des Anspruches (die Verweise beziehen sich auf dieses Dokument) soweit Anspruch 1 klar ist:

- Verfahren zum Übertragen von Daten zwischen einer mobilen ersten Einrichtung und einer von der ersten Einrichtung zumindest zweitweise entfernten Datenzentrale, wobei die Übertragung der Daten über wenigstens eine mobile erste Datenübertragungseinrichtung erfolgt (Seite 3, Zeilen 25-27),
dadurch gekennzeichnet,
 - dass die übertragenen Daten erste Daten umfassen, die durch kryptografische Mittel authentifiziert werden (Seite 3, Zeilen 27-28).
- 3. Die Merkmale des Anspruchs 1 sind ebenso in Dokument D2 (z.B. Absatz 3, Absatz 18) offenbart.
- 4. Der Anspruch 17 korrespondiert zu Anspruch 1, die Feststellungen zu Anspruch 1 gelten entsprechend. Deshalb ist Anspruch 17 nicht neu (Artikel 33(2) PCT).
- 5. Wenn, basierend auf geringfügigen Änderungen der Interpretation, Neuheit strittig wäre, wird darauf hingewiesen, daß der Gegenstand der unabhängigen Ansprüche 1 und 17 keine erfinderische Tätigkeit enthält (Artikel 33(3) PCT).
- 6. Die abhängigen Ansprüche enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf die sie sich rückbeziehen, die Erfordernisse des PCT in Bezug auf Neuheit bzw. erfinderische Tätigkeit erfüllen. Die Merkmale sind entweder in D1 offenbart (z.B. "die authentifizierten ersten Daten werden in einen Protokolldatensatz eingefügt und in der ersten Einrichtung gespeichert"), D3 (z.B. "die erste Überwachungsreaktion umfasst einen Abrechnungsvorgang"), D4 (z.B. die ersten Überwachungsdaten umfassen einen ersten Erfassungswert einer ersten Erfassungsgröße; "die ersten Überwachungsdaten werden in der Datenzentrale analysiert") oder offensichtlich für den Fachmann (z.B. "die Daten umfassen eine Zeitkennung").

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

1. Wenn neue unabhängige Ansprüche eingereicht werden, sind diese vis-à-vis D1 zu formulieren (Regel 6.3 (b) PCT).

2. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der in den Dokumenten D1-D2 offenbarte einschlägige Stand der Technik noch diese Dokumente angegeben.
3. Ein Teil des Gegenstandes der Beschreibung wird nicht von den Ansprüchen umfasst (Seite 14, Zeilen 25-34, Seite 30, Zeilen 8-11). Diese Inkonsistenz zwischen den Ansprüchen und der Beschreibung führt zu Zweifeln über den Schutzbereich und daher zur Unklarheit (Artikel 6 PCT).
4. Die verschwommene und unpräzise Angaben in der Beschreibung auf Seite 30, Zeilen 19-21 erwecken den Eindruck, daß der Gegenstand, für den Schutz begehrt wird, nicht dem in den Ansprüchen definierten Gegenstand entspricht, und führen daher zur Unklarheit (Artikel 6 PCT), wenn die Beschreibung zur Auslegung der Ansprüche herangezogen wird.
5. Der Anmelder wird gebeten, die Änderungen auf Austauschseiten wie in Regel 66.8 a) PCT vorgeschrieben einzureichen.

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

1. Die Ansprüche, die nicht den Erfordernissen des Artikel 6 PCT genügen:
 - 1.1 Der Ausdruck
 - "insbesondere", verwendet in den Ansprüchen 1, 12, 17, 29, 35; führt zu Zweifeln über den Schutzbereich (s.a. PCT Gazette, Sektion IV III-4.6), weil nicht klar ist, ob die diesem Ausdruck folgenden Merkmale zum beanspruchten Schutzbereich gehören oder nicht.
 - 1.2 Die Ausdrücke
 - "zumindest zeitweise entfernte Datenzentrale", verwendet in den Ansprüchen 1, 12, 17;
 - "ein vorgegbares Ereignis", verwendet in Anspruch 5, 21; haben keine allgemein anerkannte Bedeutung und führen daher zu Zweifeln über

den Schutzbereich der Gegenstände der jeweiligen Ansprüche.

1.3 Es ist unklar, ob mit den Begriffen

- "einer mobilen ersten Einrichtung" und "der ersten Einrichtung", verwendet in den Ansprüchen 1, 12, 17;
- "erste Daten", verwendet in Anspruch 1 und "die Daten", verwendet in Anspruch 11;

dieselbe Entität gemeint ist oder nicht.

1.4 In Anspruch 4 ist unklar, welches technische Merkmal mit dem Ausdruck "die ersten Daten zur Authentifizierung der Übertragung der ersten Daten umfassen eine Übertragungsidentifikation.

1.5 Der Ausdruck "weitere, nicht von der ersten Einrichtung übermittelte Daten", verwendet in den Ansprüchen 16 und 34 lässt den Leser im unklaren über die Bedeutung des technischen Merkmales auf das sich der Ausdruck bezieht und führt daher zu Zweifeln über den Schutzbereich.

1.6 Der Gegenstand der Ansprüche 10, 15, 27, 32, 33 ist durch das zu erreichende Ergebnis definiert und daher unklar.